NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DISTRIBUTED COMPUTING ENVIRONMENT FOR MINE WARFARE COMMAND

by

Lane L. Pritchard

June, 1993

Thesis Advisor: Myung Suh

Unclassified
Security Classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification: Unclassified

1b Restrictive Markings

2a Security Classification Authority

2b Declassification/Downgrading Schedule

3 Distribution/Availability of Report
Approved for public release; distribution is unlimited.

4 Performing Organization Report Number(s)

5 Monitoring Organization Report Number(s)

6a Name of Performing Organization
Naval Postgraduate School

6b Office Symbol (if applicable)
AS

7a Name of Monitoring Organization
Naval Postgraduate School

6c Address (city, state, and ZIP code)
Monterey CA 93943-5000

7b Address (city, state, and ZIP code)
Monterey CA 93943-5000

8a Name of Funding/Sponsoring Organization

6b Office Symbol (if applicable)

9 Procurement Instrument Identification Number

Address (city, state, and ZIP code)

10 Source of Funding Numbers

Program Element No	Project No	Task No	Work Unit Accession No

11 Title (include security classification) DISTRIBUTED COMPUTING ENVIRONMENT FOR MINE WARFARE COMMAND

12 Personal Author(s) Lane L. Pritchard

13a Type of Report
Master's Thesis

13b Time Covered
From To

14 Date of Report (year, month, day)
June 1993

15 Page Count
109

16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 Cosati Codes

Field	Group	Subgroup

18 Subject Terms (continue on reverse if necessary and identify by block number)
Distributed Computing, Information Systems Management

19 Abstract (continue on reverse if necessary and identify by block number)

The Mine Warfare Command in Charleston, South Carolina has been converting its information systems architecture from a centralized mainframe based system to a decentralized network of personal computers over the past several years. This thesis analyzes the progress of the evolution as of May of 1992. The building blocks of a distributed architecture are discussed in relation to the choices the Mine Warfare Command has made to date. Areas that need further attention and development are discussed based on the research findings. Finally, recommendation for future planning, procurement and improvements to the system are made. Lessons learned by this command during the conversion to a networked system are described.

20 Distribution/Availability of Abstract
X unclassified/unlimited _ same as report
_ DTIC users

21 Abstract Security Classification
Unclassified

22a Name of Responsible Individual
Myung Suh

22b Telephone (include Area Code)
408-656-2637

22c Office Symbol
AS/SH

83 APR edition may be used until exhausted
All other editions are obsolete

security classification of this page
Unclassified

Approved for public release; distribution is unlimited.

Distributed Computing Environment for Mine Warfare Command

by

Lane L. Pritchard
Lieutenant Commander, United States Navy
B.A., Miami University of Ohio 1978

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 1993

Author: Lane L. Pritchard
Lane L. Pritchard

Approved by:
M. Suh, Thesis Advisor

Kishe Sen Gupta
K. Sengupta, Second Reader

David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

The Mine Warfare Command in Charleston, South Carolina has been converting its information systems architecture from a centralized mainframe based system to a decentralized network of personal computers over the past several years. This thesis analyzes the progress of the evolution as of May of 1992. The building blocks of a distributed architecture are discussed in relation to the choices the Mine Warfare Command has made to date. Areas that need further attention and development are discussed based on the research findings. Finally, recommendation for future planning, procurement and improvements to the system are made. Lessons learned by this command during the conversion to a networked system are described.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. PURPOSE

In 1990 the Mine Warfare Command located in Charleston, South Carolina, decided to eliminate their mainframe computer and install a distributed computing system. This thesis will examine the process involved in making the change to a new information system architecture and make recommendations for future improvements to the system. Distributed computing will definitely play an important role in meeting information systems needs in military commands of the future. All commands will experience the need to replace existing systems with new technology. There needs to be a systematic approach to converting to a distributed environment. The content of this thesis is based on an assesment of the command information system status as of May of 1992. A variety of lessons learned at the Mine Warfare Command, and the management and technical decisions made during the conversion will be explained and discussed. These lessons should provide future commands with a list of areas to be examined before converting to new distributed systems.

B. BACKGROUND

Distributed computing is not a new topic in the information technology world. It is, however, new to many

Department of Defense commands. A variety of circumstances has recently brought information systems resources to the forefront of strategic planning for international corporations and government agencies. For businesses to remain competitive they must determine how their information systems can supply them with competitive advantage [Ref. 1]. The choices that top executives and managers make have a profound impact on the success or failure of their business. As the Department of Defense cuts budgets and downsizes due to congressional and public pressure for a peace dividend, it is examining business management practices that have worked for industry's leading corporations. The Defense Management Review Decisions (DMRD's) are an example of applying successful business methods to Department of Defense functions. The Corporate Information Management (CIM) initiative is examining the possibility of consolidation and standardization of information systems to eliminate duplication and waste. The decentralization of information systems assets is one of these current management trends in industry and government. There is an increasing pressure to modernize equipment and systems while improving productivity and generating cost savings.

Buchanan and Linowes described a method of evaluating the appropriate degree of decentralization for specific computer systems in several Harvard Business Review articles in 1980 [Ref. 2 & 3]. At that time decentralization and distributed computing were considered to be new trends and an alternative with which general managers needed to be familiar in order to position their business for competition. Now in the early 1990's it has become critical for managers to understand information system resources and take advantage of their ability to be able to process information from a variety of locations, to eliminate duplication of effort, and to reduce information systems budgets.

Distributed data processing (DDP) initially became possible due to improvements in integrated circuit and communication technology, and the subsequent decrease in hardware costs. Until the 1970s Grosch's Law (which posits that the cost per machine instruction executed is inversely proportional to the square of the machine power) supported the centralization of automated data processing (ADP) assets due to cost [Ref. 4]. This required one large central repository for equipment and data.

The progressive change in hardware cost and increase in capability have also led to changes in programming philosophy. Data was no longer part of the programming structure. It was held separately and accessed by the program. This separation of program and data gave additional flexibiiity to the uses of data and the possibility of decentralizing data processing for some applications.

End users were creating pressure on ADP managers to change the way in which data processing was conducted. This pressure was due to frustration with data center priority systems, administrative red tape, lack of understanding of costs, and immense project backlogs. The design and planning of systems now involve the end user to a great extent. The advantages of DDP mean that different groups of users can have totally different interfaces to the same systems and receive different outputs. User involvement can complicate the development process as user requirements change often and are sometimes technically impossible. This leads to long delays and cost overruns for poorly managed projects. However, managers of independent divisions with entrepreneurial influences have a strong desire to control the critical information data processing can supply and that determine success or failure in the corporation [Ref. 1].

DDP can be described in a variety of ways. One commonly held notion is that DDP is the distribution of hardware around an organization, but it involves much more than hardware. DDP requires choices about the placement, control and interaction of hardware, software, data, tasks and personnel [Ref. 5]. Early DDP was simply the distribution of computer terminals with online access to a centralized database around an organization, thereby facilitating transaction processing. The current DDP makes it possible to distribute data all over the world, while allowing personnel in those locations to work on the same task and communicate on a real time basis.

The advantages of this flexibility are tremendous. Rapid access to a distributed data through real-time communication channels eliminates the need for extensive travel and the ensuing high budget for travel, mail, and overnight delivery charges. Personnel morale has been noted to improve as a result of easier and more efficient ways to perform tasks [Ref. 1]. Unfortunately, the possibility for error is also high. Data may be corrupted, hardware and software may be duplicated, personnel may fail to communicate and coordinate, and competitive advantage may be lost.

C. MINE WARFARE COMMAND

The trend toward information processing on distributed computer systems and networks is already well underway in corporate America, and Department of Defense activities are quickly following suit. Reasons for this vary from activity to activity, but most involve some pressure to modernize equipment and generate cost savings at the same time. Interest is being shown in incremental modernization with lower cost per step than wholesale replacement of massively expensive mainframe components.

The Mine Warfare Command (MWC) in Charleston, South Carolina is one of the commands that has chosen this path. Five years ago the only computing power was the mainframe. Specialized programs to support the mine warfare mission were written in FORTRAN and run on the mainframe. As the command acquired personal computers (PC's) more and more time was spent by the programmers and analysts developing special PC programs for small groups of personnel in each department. Several years ago the command reduced its dedicated Data Processing staff to only those personnel required to operate the mainframe, placing all of the programmers and analysts in the customer departments to provide direct support. Each department is now responsible for planning and developing its own programs and processing. This dispersion of personnel has helped the departments achieve time and money saving, but has led to the lack of a coordinated command level plan. Equipment has been procured and networks installed independently. The command now has Macintosh's, IBM PC's or clones running DOS, and a few Sun Microsystems SPARC workstations running the UNIX operating system. Several departments have their own networks. Some of the networks have been connected using an Ethernet backbone. Each of the command's mainframe programs is being converted to run on one of these microcomputer platforms. The maintenance contract for the mainframe ended on 1 October 1992 and will not be renewed.

This sequence of events has caused the command to move away from mainframe computing, but has not actually produced a distributed computing environment in the strict sense. Data is not shared and processes are not cooperating. Unnecessary costs and duplication of effort between departments are apparent. The technology to connect these diverse platforms into a seamless network exists. The command, however, does not have anyone with a CIM perspective directing its overall development or planning for future connectivity.

MWC's request for analysis of current utilization, and recommendations for future plans and procurement is a first step in the direction of a truly distributed computing environment.

D. RESEARCH SCOPE

The primary objective of Commander, Mine Warfare Command is to determine the types of hardware and software that should be procured now and in future years to support mission functions on a distributed network of diverse platforms. The command wanted to verify that their network architecture and planned implementation made sense based on existing technology. They also required some assessment of which types of developing technology are compatible with current equipment configurations and would support future projected utilization levels. The management policy for information systems must also be examined and revised to support both internal and external organizational changes.

This thesis will provide a variety of lessons learned for other Department of Defense commands planning to move toward distributed computing. This will help to eliminate repeating the same mistakes and unnecessarily using scarce information systems funding and resources.

E. RESEARCH METHODOLOGY

Mine Warfare Command is a relatively small command contained in one building and staffed by approximately 80 personnel. The command specific structure, missions and goals will be described in Chapter II. Due to the small size of the command the primary data collection method used was a combination of questionnaire, onsite interview and personal observation. The questionnaire, included in Appendix A, was distributed to all command personnel. It assessed utilization of current assets and prospective needs. Onsite interviews were conducted with each department head, the chief of staff and an information systems representative from each department. A list of the questions posed to these individuals is provided in Appendix B. Onsite observations were used to determine compliance with written instructions, the extent of the information system plans documented in writing and whether currently written development plans are progressing as documented in the command's Component Information Management Plan (CIMP) [Ref. 6].

F. THESIS OUTLINE

This thesis is divided into five chapters. Chapter II describes the current system at the Mine Warfare Command (MWC) including their command organization and mission, and the evolution of their information system architecture. Chapter III discusses the building blocks for a distributed computing system. Chapter IV explains the requirements of MWC in light of the building blocks and current IS management principles. The fifth chapter provides recommendations for future procurements and management of the system.

II. DESCRIPTION OF CURRENT SYSTEM

A. MINE WARFARE COMMAND: MISSIONS AND STRUCTURE

During the 1980's the Mine Warfare Command (MWC) was a small staff command reporting directly to the Chief of Naval Operations. Due to the interest in and growth of the importance of mine warfare in world events, MWC became, on 1 October 1991, an operational type commander with responsibility for all tactical mine warfare resources on both the East and West coasts. Previously, these units had been assigned to the Surface Force Type Commanders, and the MWC staff supported the Chief of Naval Operations solely with data analysis and as an assistance liaison with operational forces. New responsibilities include all previous services and the addition of commanding operational mining and mine countermeasures forces. The command collects, maintains, stores and analyzes data on all aspects of mine warfare for the United States and several allied navies. New tasks include administration and maintenance of force readiness, and inspection and support functions. Analysis of data and development of new tactics in mine warfare require the creation of a variety of graphical presentations incorporating nautical chart images. A large portion of this data is obtained from satellite photos and is classified confidential or above.

1. Mission and Goals

Commander, Mine Warfare Command's (CMWC) specific mission and functions are assigned in OPNAVINST 3370.3B. CMWC's general responsibility is to support the fleet Commander in Chiefs and the Chief of Naval Operations by assuring the readiness of fleet mine warfare units, plans, forces and assets. Within this broad mission there are six functions summarized below:

a. Support of Operational Units

Administrative and budgetary support of all Naval Mine Warfare assets including the Mine Groups and Divisions (the minesweeping boats and new MCM ship class) and the helicopter squadrons which perform minesweeping operations. All of these assets are being positioned at Engleside, Texas over the next several years.

b. Mine Warfare Planning and Mine Warfare Systems Evaluation

CMWC is responsible for the preparation and maintenance of fleet mine warfare (mining and mine countermeasures) plans for war, contingency and exercise operations, and the analytical evaluation of current and developmental mine warfare systems.

c. Fleet Mine Readiness Management

CMWC in conjunction with Commander, Mobile Mine Assembly Group (COMOMAG) is responsible for the readiness and availability of fleet mine stocks in support of war plans.

d. Fleet Mine Warfare Tactics

CMWC is responsible for initiating actions to develop and recommend revision to existing tactics for fleet mining and mine countermeasures forces.

e. Fleet Route Survey

CMWC is responsible, as the CNO Route Survey Program Coordinator, to oversee the development of the Route Survey Program as a mine countermeasures risk reducing initiative. Within this mission area is the requirement for a Route Survey Data Management System (RSDMS).

f. Mine Warfare Readiness Certification Inspection Program

CMWC, via the Inspection Group, is responsible for assessing the mine warfare readiness of all fleet unites assigned a mine warfare mission.

Of these missions areas each requires Information System (IS) resources support, with several requiring detailed databases to hold historical data obtained during inspections or exercise results. The Route Survey Program requires a sophisticated database to maintain a large amount of meteorological and navigation data which is updated and accessed continuously by fleet inputs and mission planning requirements. Budgetary support requires spreadsheet and financial applications. Tracking the status of on hand mine inventories requires a database which will interact with logistics commands and inventory control programs. Additionally, the expanded missions areas require increased word processing support and enhanced communication abilities. The most ambitious command software development projects include the development of a Decision Support System to support the Fleet Mine Warfare Tactics mission and a Geo-Operational Planning and Assessment System (GOPAS) to allow the automated generation and printing of minefield planning folders. *Historically, tactical* decisions were made and documented in plans or reports. Follow on planning by different individuals required reading the previous reports, plans, and results and adapting them to create new plans consistent with previous plans and current tactics. A database of plans and tactics and a DSS to assist with the generation of new plans will improve consistency and increase confidence in staff directives.

The current command goals are to improve fleet support in all mission areas. The United States mine forces, since World War II, have been predominantly thought of as coastal defense units. Restructuring the mine forces under the new CMWC authority was primarily undertaken to ensure that specific numbers and types of mine warfare assets would be available to deploy anywhere in the world on short notice. It is critical for the command to be able to do more with less, and improved computer resources are a cost effective way to provide the added performance necessary. Budgets are not decreasing for this command as rapidly as they are for other sections of the military, but an overall reduction in funds will require that available resources be maximized, especially computing capabilities. International events over the past several years have served to bring the capability of the United States mine forces to the forefront of concern for both senior military officers and foreign affairs policy makers. A CMWC department head stated "We are one of the few areas of defense that is now considered a growth industry."

2. Organizational Structure

The command is staffed by eighty Department of Navy personnel, military and civilian, and located on the waterfront of the Charleston Naval Base. The Commanding Officer is a Rear Admiral supported by seven Commander or Captain department heads. Subordinate commands include the Mobile Mine Assembly Group (COMOMAG), the Commander Mine Warfare Inspection Group (COMINEWARINSGRU), and the operational forces Commander Mine Groups One and Two.

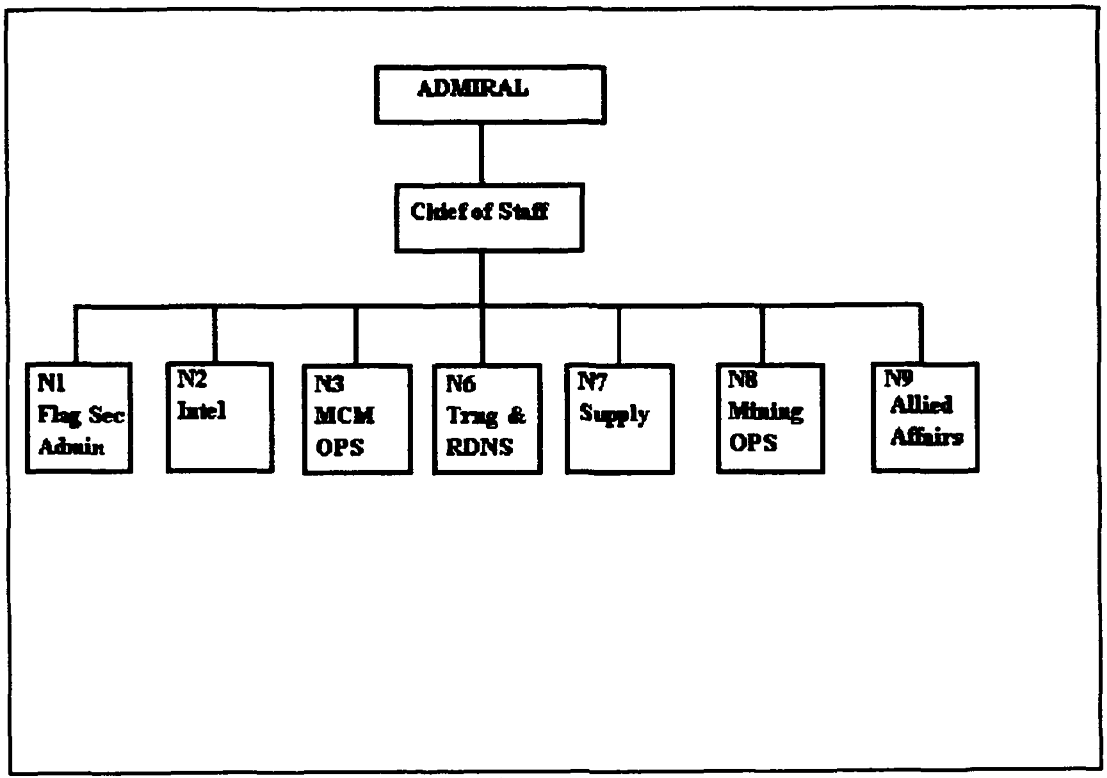

Figure 1 : CMWC Organization Chart

Figure 1 shows the organizational structure of MWC in early 1992. Each of the departments may have several sections. The function of each department is described below:

a. Administration - N1

This department includes divisions for administration, classified material control, communications, security, information systems and several specialized administrative aides for programs like drug and alcohol programs and career counseling.

b. Intelligence - N2

The Intelligence department consists of a few personnel who collect and maintain Mine Warfare related intelligence information necessary to support mission and tactical planning.

c. Mine Counter Measures Operations - N3

This department is one of the largest and is responsible for the primary mission area of mine countermeasures. It is headed by a Navy commander and contains divisions for systems analysis, exercise analysis and tactics, plans and systems development. This group is responsible for support and interaction with the operational units both air and sea.

d. Training and Readiness - N6

A small group responsible for maintaining training plans and documenting accomplishments. Tracking fleet readiness based on training conducted is critical to exercise and mission planning. This department is broken down into segments to track aviation, damage control, engineering and combat systems training needs and schools.

e. Comptroller - N7

This department functions as the supply department for the command coordinating all requisitioning, procurement and budget management.

f. Mining Operations - N8

The Mining Department is also headed by a Commander and is the other large department in CMWC. This department is responsible for the Route Survey database and puts together mining plans for all areas of the world. Tactics and doctrines for mining are also studied and prepared. The department is broken into segments based on areas of the world (i.e. Atlantic, Pacific, European, etc.).

g. Allied Affairs - N9

Allied Affairs works with all NATO countries in planning mine warfare exercises and doctrine. This group interacts with all the other departments at CMWC to ensure the proper support for overseas mine warfare operations.

B. EVOLUTION OF INFORMATION SYSTEMS ARCHITECTURE

This section describes the history of the major milestones in the computer architecture changes at CMWC over the past 10 years until approximately January 1992. A variety of reorganizations and changes in top level management strongly influenced the direction of evolution in computer resources.

The mission of CMWC created an early need for large databases of geographical information containing classified data. In the 1970's database applications were written to support CMWC's mission requirements. Their original computer was a Gould Cell 32/55. A VAX mainframe was acquired in 1984 to hold the growing database and allow processing via hardwired dumb terminals. The first application was the Route Survey program which consolidated information collected by fleet units for future use during Mine Countermeasures missions. The DECNET operating system was used for connectivity with terminals in various offices. The second application developed was for inventory control of the stock of mines maintained by CMWC's subordinate command COMOMAG. Its database held mine numbering and capability information. It also created Mine Labels and Mine Capability Plans & Reports.

Both of these original applications were written in Vax Fortran Native Code and are considered Mission Critical Modeling Programs. CMWC system development is supported by the Naval Research Laboratory in White Oak, Mississippi. CMWC contracts with this organization for software development and then maintains its own staff of analysts and programmers for maintenance and upgrade.

In 1987 these applications ran on a VAX 11/780 mainframe with a 1 MIPS capability running the VMS operating system Version 2. A VAX All-in-One Office Automation Minicomputer Model 8350 with 1.7 MIPS of processing power was obtained in 1986 to support the need for coordinated word processing and electronic mail. The All-in-One software included a spreadsheet, time and calendar management models. Additional remote terminals were installed for administrative personnel. Most department heads also had VAX terminals at their desktop.

This equipment and software required costly periodic upgrades to the hardware and operating system software. Continuous coverage hardware maintenance contracts added significantly to the yearly Information System (IS) budget.

In the 1988 and 1989 time frame the command began to acquire a number of Zenith 248's for individual computer applications. Several Macintosh computers were bought to produce the graphics presentations required for briefing the CNO and his staff. One of the Department Heads (a Navy Captain) was interested in acquiring additional Macintosh computers and networking these in his department. A system called the Personal Computer System Architecture was purchased and installed on the VAX allowing personal computers to store files on the VAX in native mode. The supply department developed elaborate spreadsheets for tracking budget data on IBM compatible 286 PC's and were able to store this *information on the VAX disk drives.* A program called PACER was acquired to provide the same capability for the Macintosh.

This information system architecture was supported by a staff of about 10 civilian analysts and programmers and seven enlisted Data Processing technicians who operated the VAX mainframe and peripheral equipment. The group was headed by a civilian GS-13 level manager who reported to the Supply Officer (Command Comptroller), a Navy Commander.

The IS organization was that of a standard data processing organization with centralized hardware and applications. The IS manager reported to the Financial branch head and the IS staff was isolated from the rest of the command. User requests for changes and upgrades to programs and systems took a lot of time as the Fortran applications required extensive rewriting.

The manager of the group was kept appraised of improving technology and submitted proposals for acquisitions to improve the processing systems. He kept tight control of what types of hardware and software were purchased. The IS resources were centralized and users were in most cases told what they needed (hardware and software) to perform their mission and improve their productivity. The users at the command became disgruntled with their data processing support especially in light of exciting advances in computer technology appearing commercially. Many of the personnel at CMWC became PC "literate" and increased the pressure for improved computing capabilities.

In the summer of 1989 significant changes occurred that resulted in the command's current organizational structure, and decisions were made that led to the change in their IS architecture. The long time head of Information Systems left the command for another position. Concurrently, a proposal was submitted by the IS department to upgrade the VAX hardware to the new VAX 4000 model to support networked PC's and Macintoshes. Without the strong influence of the departed IS manager the decision was made not to upgrade the VAX, but instead to purchase additional Macintoshes and peripheral equipment and connect them in a network as proposed by one of the Department Heads. During 1990 and 1991 the additional equipment, software and hardware was bought and installed. The Information Systems department was reorganized, and the analysts and programmers were assigned to individual department heads. The decision was made to phase out the mainframe over a period of several years. Pursuing the path to a totally networked architecture without a mainframe was started, but without a clear plan for implementation. Each department head determined his department's data processing needs, requested and lobbied for the necessary equipment, and built his support structure independently. Departments began to evolve networks and computer capabilities based on the interest level of the senior officer in various computer types and technologies rather than on a well thought out plan. Hardware and software upgrades for the VAX mainframe equipment were cancelled so that the money could be used to procure network equipment and PC's.

Personnel continued to use the VAX for the two mission critical programs and word processing. The IS department strove to support the ever increasing scope of hardware and software products used by various groups. A contract was established with the Naval Research Lab at White Oak to rewrite the mission critical applications for the SUN Workstations. The command's enlisted data processing technician billets were released as they were no longer needed to run the mainframe equipment.

It is clear that the rapid changes in computer architecture at the command stem from several causes. The loss of a strong manager who supported centralized IS services and controlled procurement, and an increasing number of users with interests in new computer technology. Eliminating the expenses for the VAX mainframe increased the commands flexibility to purchase and try out new equipment, but led to such a diverse number of hardware platforms and software packages the decreased staff could no longer provide support.

An ADP Steering Committee was formed to get the command's information systems planning and procurement under control. An Ethernet installation plan to connect the entire command was drawn up and equipment ordered to fill in gaps in the distribution of PC's and acquire adequate numbers of legal software packages. The network plan added wiring to connect the various departmental networks to a central file server. Most of this equipment was ordered on the DESKTOP III contract, but never delivered. The purchase order was cancelled, rewritten and finally procured locally in several batches of equipment. The command was reorganized to support the new Type Commander mission requirements and the IS Division was placed in the Administrative Department reporting to a line Lieutenant Commander. In 1991, some steps to bring IS software development under control were detailed in a software development plan called a Component Information Management Plan (CIMP) [Ref. 6]. This sequence of events solved some of the IS management problems, but led to others that will be discussed in later chapters.

C. CURRENT ARCHITECTURE

The computer architecture at CMWC as of May 1992 consisted of the VAX mainframe equipment described in the previous section and the VAX All-in-One office automation system, about 30 VAX terminals, 25 Macintoshes, 25 PC's (IBM compatibles of different brand names), a few laptop PC's, and 3 SUN UNIX Workstations. This combination of equipment was interconnected at several points. A 386 PC was set up as a file server using NOVELL Netware 3.0 as the network operating system linking several PC's. One department had a Macintosh network running the Apple Local Talk operating system. This Macintosh network was connected to an Ethernet LAN and then to the mainframe to provide access to printers and plotters. Figure 2 depicts the connectivity of this disjointed, initial network.

The Ethernet network wiring was installed by the command IS personnel, running to all locations where the command plans to place PC's. Over 30 PC's, software, and peripheral equipment have been on order for over a year. Departments with both Macintosh and IBM compatible PC's are running dual networks with Apple Local Talk connecting the Macintoshes and

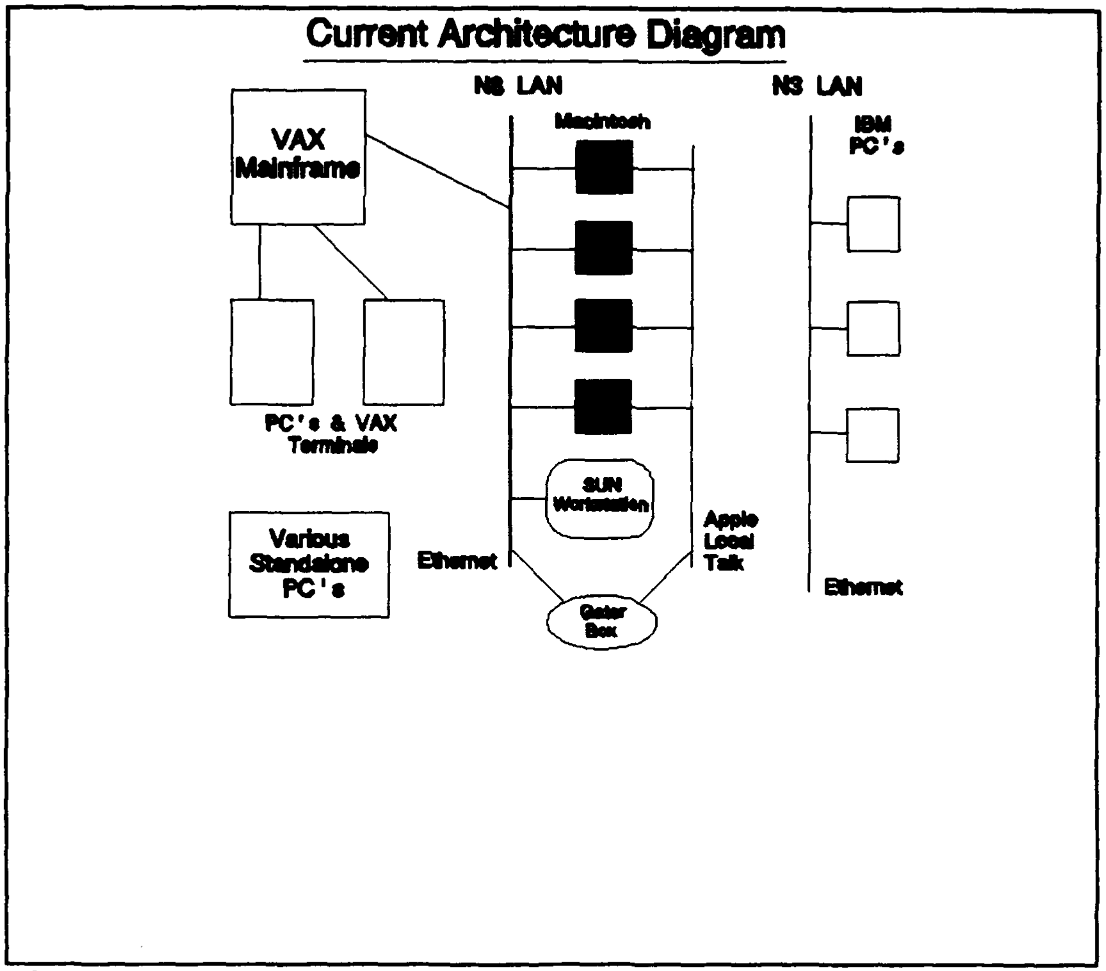

Figure 2: CMWC LAN Architecture as of MAY 1992

a Gator Box Bridge facilitating transmissions to the PC's on the Ethernet network wiring running Netware.

The maintenance contract for the remaining VAX hardware expired on 1 October 1992 and was not renewed. The VAX 11/780 is now on the Department of Defense (DOD) obsolete equipment list. The only maintenance contracts the command holds are for a few color printers. They do their own PC and network maintenance, and use one time repair contracts if they cannot fix the equipment. Most of the new PC's are covered by 1 to 3 year warranties.

In order to assess this command's future IS architecture and procurement needs a baseline analysis must be done to establish where they stand in their development of a distributed computing architecture. The next chapter will describe the basic building blocks of a distributed computing system.

III. ARCHITECTURE FOR DISTRIBUTED COMPUTING

> A strategy to take advantage of distributed computing must be planned and documented by all participants. The objective of the strategy should be to establish a framework within which distributed processing can grow rapidly, with maximum user involvement, with high productivity of application development, without the pitfalls...

This quote from James Martin's book on Design and Strategy for Distributed Data Processing [Ref. 5] proposes that there are different aspects of the management of systems which can be centralized or distributed. The primary ones are:

- The setting of standards
- The selection of architectures
- The selection of hardware and software
- Usage decisions - selection of projects and feasibility studies
- The design of data - data base administration and control
- Application development

> What is best for one organization may be different from that which is best for another. Organizations differ greatly in their management style and structure. However, some management patterns for distributed processing are more likely to bring success than others. Perhaps the greatest danger of distributed processing and minicomputers is that incompatible systems will spread at a rapid rate through an organization. They cannot be easily hooked together at a later time.

CMWC's situation as described in Chapter II has come close to paralleling this dire prediction. Luckily, there has been some acknowledgement of standards and the need to procure equipment that complies with the "open systems" ideal allowing connectivity between diverse equipment. The next several sections will explain the management aspects referred to by Martin available to CMWC for standards, architecture, hardware, software and applications.

A. STANDARDS FOR OPEN SYSTEMS

The first chapter described some of the technological advancements and trends that allowed the concept of distributed computing to develop. First, a distributed computing system has hardware, software and data distributed around an organization to various places, thereby allowing people to access the data regardless of where they are located, and communicate with other users. CMWC has this scenario and the requirement to make it work to perform their mission. Second, distributed computing was made possitle by advances in telecommunication technology which allow the formation of networks, and transfer of data and processes over these networks. To apply these requirements to a diverse set of hardware and software requires a well defined set of communications protocols. Protocols enable diverse types of equipment to communicate through a series of agreed upon processes.

The following sections describe the major standards and protocols that CMWC may utilize to formulate a distributed architecture.

1. OSI Model

The details of the communication protocols and versatility of distributed computing lie in the network architecture commonly referred to as the Open Systems Interface (OSI) Model. The OSI Model was developed by the International Standards Organization (ISO) and is a framework for defining standards for linking heterogenous computers [Ref. 7]. The OSI Model is implemented in seven layers. Each layer defines functions that protocols developed for that layer will perform. These functions may be implemented in any way the designer wishes as long as they comply with the standards and allow connectivity to the layers above and below. The model divides communication architecture into seven layers and provides a logical decomposition of the complex problems associated with interconnection of diverse computer hardware. Each of the layers provides services to the next higher layer. The layer and functions of the OSI Model are described in Reference 7 as follows:

> 1. Physical - designates physical interface between the devices on the network and the rules for the transfer of an unstructured stream of data bits (bit encoding) over a physical medium (cable). It deals with the mechanical, electrical, functional and procedural characteristics to access physical media.
>
> 2. Data Link - provides the reliable transfer of information across the physical link. It designates the assembly of data bits into packets of information to be transmitted, and adds addressing information and error checking (synchronization, error and flow control) to be used across a single link.
>
> 3. Network - responsible for establishing, maintaining and terminating connections. Determines the path that data packets take across a network based on destination and routing information and provides upper layers with independence from the data transmission and switching technologies used to connect systems.
>
> 4. Transport - provides reliable, transparent transfer of data between end points and provides end to end error recovery and flow control across more than one link.
>
> 5. Session - control structure for communication between applications. It establishes, manages, and terminates connections between cooperation applications.
>
> 6. Presentation - provides independence to the application processes from differences in data representation (syntax) and encryption or compression schemes.
>
> 7. Application - provides access to the entire OSI environment for users on network and provides the distributed information services like electronic mail, file transfer, etc.

2. DOD Model

An alternative model in use by industry is similar to the OSI model but condenses the seven layers down to four. The layers in this model consist of:

1. Network Access Protocol (NAP) Layer - this contains the protocols for the same first three layers of the OSI Model, the Physical, Data Link and Network Layers.

2. Internet Protocol (IP) Layer - this fits between the OSI Layers 3 and 4 (OSI has incorporated this into Layer 3), and consists of procedures required to allow data to traverse multiple networks between hosts, usually by providing a routing function in network gateways [Ref. 7].

3. Transmission Control Protocol (TCP) Layer - is equivalent to the Transport Layer in OSI Model.

4. Upper Layer - incorporates the top three layers of the OSI Model, the Session, Presentation and Application Layers.

This architecture is called the DOD Model because of its original inception by DOD in constructing the Internet (a diverse network connecting government agencies, universities and corporations). This model is usually referred to in industry literature as Transmission Control Protocol/Internet Protocol (TCP/IP) and significant controversy has been in the press recently concerning the government's desire to embrace the OSI standard instead of the architecture that it originally created. Figure 3 depicts the OSI and DOD Model Layers.

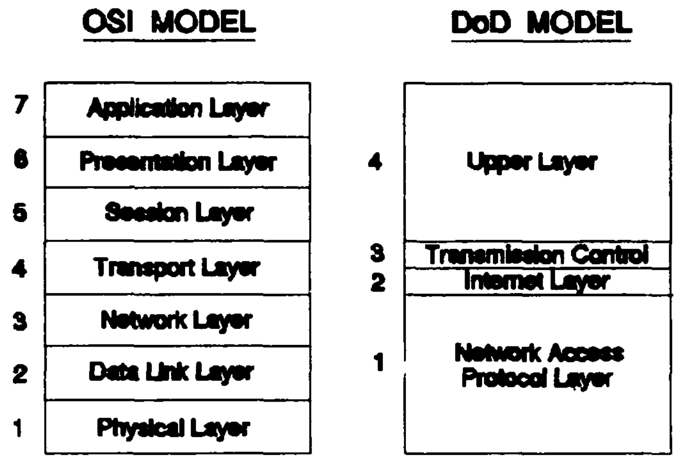

Figure 3: OSI & DOD Protocol Layer Models

3. Government Open Systems Interconnection Profile

The Government Open Systems Interconnection Profile (GOSIP) provides implementation specifications and is the standard reference for all Federal Government agencies to use when acquiring IS or communication equipment or services to ensure compliance with the ISO/OSI Model standards [Ref. 8]. The proliferation of diverse IS products and the need to exchange information between them led the United States government to promote the acquisition of open systems to meet information processing requirements. It addresses the need for the government to move to multi-vendor interconnectivity without sacrificing essential functionality already implemented in systems [Ref. 9]. As of August of 1990 it is a mandatory requirement with which all IS acquisitions must comply. GOSIP is a dynamic profile which specifies a selection of protocols that may be used at each layer of the OSI Model. In this way it is more restrictive than the two models mentioned in the paragraphs above by mandating specific protocols not just functionality. It will be updated as higher level protocols continue to evolve.

CMWC has complied with the GOSIP standard by choosing a combination of the Ethernet bus thin and thick wire protocols (IEEE 802.2 for Logical Link control and IEEE 802.3 as physical medium and medium access control) in their physical network implementation. Once these protocols have been chosen, and equipment bought and installed, future network decisions must continue to comply with this choice of architecture and standards. Further hardware and software acquisition must be directed toward products which implement the protocols listed in the GOSIP standard. The specific details of CMWC's network architecture plan will be described in Chapter IV and recommendations for continued compliance in Chapter V.

B. MEANS OF CONNECTIVITY

A number of references describe the different types of LAN topologies: bus, ring and star implementations, and physical mediums available for use: shielded and unshielded twisted pair, base and broad band coaxial cable, and optical fiber [Ref. 4,5,7,& 8]. CMWC has chosen a bus wiring architecture for its Local Area Networks (LANs) using baseband coaxial cable as a backbone network and unshielded twisted pair for the individual department networks. Individual networks can be connected in a variety of ways to provide internetworking over a distance, between homogeneous networks and between heterogeneous networks. Internetworking may involve one or more of the following devices:

- **Repeaters**

Repeaters are used to interconnect LAN segments. In Ethernet, for example, the length of each cable segment can be at most 500 meters long. A maximum of four repeaters can be used to extend the network to a total length of 2500 meters. If the telecommunications signal must travel further than 500 meters in any segment the signal will become too degraded to be received properly at the destination. Each repeater in the line regenerates the signal. Repeaters are the least expensive means of extending a networks length. Computers on different sections of the network can access each other as if the cable was one continuous length.

- **Bridges**

Bridges are used to connect sections of a network that use the same architecture and protocols (homogenous LANs), but are more expensive than repeaters due to their increased capability. Bridges will not only regenerate the signal, but also filter and buffer the signal improving the chances that the signal will be correctly received at the destination. Bridges can connect networks, making a routing decision as to which network the signal should be forwarded. Bridges allow for protection between networks by compartmentalization and do not allow unrestricted access to the computers on another network as do repeaters. A bridge might also be used where only a repeater was actually needed to provide the network more reliability. If one section of the network goes down the others will still operate if they are connected by a bridge. This is not true of repeaters.

- **Gateways**

Gateways are used to connect heterogeneous LANs. They provide the same capabilities as bridges but in addition they will translate a message from one network protocol to another.

CMWC uses all three of these devices. It uses repeaters to extend the length of its network, it uses bridges to connect the departmental networks onto the backbone and provide access to the file server, and it uses gateways to connect the dissimilar PC and Macintosh networks which use different messageing formats.

In addition to its internal internetworking requirements all government agencies will be required to connect their own networks to a Wide Area Network (WAN) within the next several years. As government moves quickly to paperless reporting systems commands will have to connect to the Defense Data Network (DDN) to download directives and upload reports. Connection to DDN requires a gateway computer with a network card running the DDN protocols connecting and translated to the commands own network protocols. CMWC does not yet have a specific requirement to connect to DDN so this connectivity will be addressed in the recommendations for future procurement. Further discussion of the advantages and disadvantages of these architectures and hardware choices will be provided in Chapter V.

C. DISTRIBUTED APPLICATIONS

Once the connectivity amoung distributed computing platforms is established, a decision must be made as to what applications will be used in a distributed manner. Standard distributed applications used on networks are electronic mail, remote data access, file transfer and storage. These applications must be supported by a network operating system usually installed on a file server with access to all portions of the network. The goal of the network is to allow the sharing of resources.

All distributed applications, including electronic mail, file transfer, distributed file systems and distributed database systems, work on the client/server model. This model divides the distributed application into two parts, one part residing on each of the two computers communicating during the distributed process [Ref. 10]. The client server principle may be implemented in one of two schemes depending on how client and server processes are assigned to distributed computing platforms. In a server-based scheme processes are run only on the "server computer". The philosophy behind this is individual PCs are clients that need services from the server. The second scheme is a peer to peer LAN in which any PC or workstation can act as a client or a server for any other workstation on the network. In this situation any workstation can designate directories on its hard drive or attached peripherals as network devices that may be used by others. A centralized design with all PCs acting as workstations accessing a central server is not as flexible as a peer to peer LAN but is more controllable, secure and less complicated for inexperienced users.

The network operating systems (NOS) vary a great deal in their abilities and qualities. The NOS is the primary building block for LANs and determines the flexibility of the network for supporting applications. It also creates a road map that users must follow when making decisions on types of server and client hardware and add on software products [Ref. 11]. The type of NOS chosen determines how much memory will be available on both clients and servers to run other applications. Various NOS's differ a great deal in how much system memory is required to run the client portion. Another consideration is ease of maintenance. Complicated NOS's require full time system administrators to keep the system running and configured properly so that all users will be productive.

CMWC chose Novell Netware 3.0 as its NOS. Its server programs run on Novell's proprietary operating system, while clients operate on a wide diversity of platforms running other operating systems. Netware is best suited for small to large single site LANs ranging in size from 20 to 250 users that require high fault tolerance and fast server to workstation communications [Ref. 11].

CMWC needs to be able to communicate across diverse networks via electronic mail. CMWC's goal is for all users to be able to send and receive electronic mail across the network. They are using the electronic mail package CC:Mail. CC:Mail was recently acquired by the large software company Lotus Development. Lotus has supported the open systems idea and has created network compatible versions of CC:Mail that run on a variety of operating systems including all of those in use at CMWC - UNIX, DOS, Macintosh operating system, etc.

Early choices of products from vendors that have been industry leaders in the open systems arena leads to easier and less expensive transition to more complex network requirements in the future.

The other major distributed application CMWC needs to utilize on its network is document management. Individual personnel have the need to create and store word processing documents. These documents are typically routed to a variety of personnel for approval and the ability to transfer files across the network will go a long ways toward eliminating the mass of paperwork that flows through the command on a daily basis. It will also eliminate lost correspondence and the resulting panic that command personnel deal with to try to finalize correspondence. Another use for shared text documents is the publication of command instructions and notices. The network file server provides easy access for all personnel and a decrease in the amount of paper stored in file cabinets and binders.

As command personnel become adjusted to utilizing the network for electronic mail and text files they will think of additional uses for the network and will branch into other distributed applications. Some other distributed uses are mentioned in Appendix C, the commands draft office automation plan.

IV. MANAGEMENT CHALLENGES

CMWC has made decisions about some of the basic building blocks of a distributed network computing system. However, an analysis of the information gathered during the onsite visit in May of 1992 revealed the following areas that should be of concern to management. Specifically, some basic IS management requirements must be addressed to provide for a future system that will support the command adequately. Most of the information revealed the following IS management ιreas that need attention and further planning. Specific details of technological hardware and software questions were addressed with the IS staff and resolved via discussion and are not included in this review.

A. COMMAND STRATEGIC PLAN FOR INFORMATION SYSTEMS

A tremendous number of excellent ideas and plans exist in different stages of development at CMWC. Unfortunately, most of these plans are in individuals minds and have not been documented in writing. Most of what is documented are equipment layout diagrams, and procurement and budget proposals. Many have been articulated at ADP Executive Steering committee meetings, and have been tentatively agreed to by upper management. Since the plans are not written they tend to be changed often as new alternatives become available. New technology is advancing so rapidly in the field of network computing that every month an appealing new option appears on the horizon. The amount of information in writing in itself is not an adequate command strategic plan. It must be consolidated and coordinated.

The current architecture and plan was outlined in Chapter II. The major emphasis of the plan is to eliminate the VAX mainframe and interconnect all command personnel through a network of diverse workstation components. This goal and the specific needs of each department should be put in writing.

A complete written strategic plan is recommended that not only encompasses software development plans, but also the hardware and peripheral equipment that is currently known to be needed to support the command applications.

The current CIMP [Ref. 6] was well written and thought out, but needs updating to reflect the changes in mission and strategic direction at CMWC that have occurred since 1991. Most importantly, this plan needs to be written and coordinated by all of the ADP analysts and programmers at the command, not written in separate pieces for various departments. The budgetary planning in particular should be consolidated as several platforms and program requirements may support the same type of work. Duplication of effort in acquiring hardware, software and actual programming should be taken into account and avoided in the future to reduce costs.

A better CIMP would include not only software development plans, but also plans for hardware, peripherals, personnel, and maintenance and upgrade of software, hardware and the network. Any plan such as this must deal with the organizational culture, the current planning process of the organization, different technologies, and how critical IS activities are to achieving goals [Ref. 1]. Environmental pressures that require this type of planning include the rapid change in technology, scarcity of personnel trained in the new technologies and the scarcity of resources in general, particularly money. Reference 1 suggests a planning process include several phases:

1. Technology Identification and Investment - includes identification of the appropriate technology to support goals, the preparation of the site, development of staff skills, and development of pilot applications using the technology.

2. Technology Learning and Adaption - develop potential users' consciousness of the existence of new technologies existence and the type of problems they can solve.

3. Rationalization/Management Control - set appropriate limits on the types of applications developed and ensure they are implemented cost efficiently.

4. Maturity/Widespread Technology Transfer - transferring developed technologies to a wider spectrum of applications in the organization.

Often all four of these phases are present in different segments of the organization. When this study began CMWC was in the first phase and over the past 9 months has passed into the second phase. The critical third stage of management control must now be implemented.

Managers must also realize that planning is not a solution to all IS problems. It does have its limitations. Personnel involved in a complex planning process are not available for other work requirements [Ref. 1]. Extensive planning and documentation may be so foreign to the organizational culture that it is disruptive to the major work flow. It can become so labor intensive that people give up and do not finish with any product to show for their efforts. If decisions are not made promptly with the knowledge available, planning does not move forward. The volatility of the environment can make plans antiquated rapidly. Extensive planning may also stifle creative views for future technology.

B. OFFICE AUTOMATION PLAN

As CMWC evolves its network installation and technology, and moves closer to the control phase it will need to establish an office automation plan. For the past several years departments have independently purchased the hardware and software that they needed as budgets allowed. As presented in Chapter II the command structure encompasses a wide range of departments, missions, databases and personnel and presents a complex problem to integrate via office automation. In an environment with a distributed architecture more care must be taken to acquire assets that complement existing resources. Interoperability of equipment and software for all segments of the organization is now critical. The need to control this aspect can be resolved by a command office automation plan.

The command survey (Appendix A) was constructed primarily to analyze the office automation requirements at the command. Eighty percent of the surveys were returned showing that 99% of the command personnel require some type of office automation to perform their job. Some personnel still use a typewriter one day a week primarily to type envelopes, forms and memo's. This result points to a need for electronic mail, print merge features for mailing envelopes and online automated forms for a variety of purposes. Specifically, the first priority should be to automate the filing of travel claim forms as this was mentioned repeatedly.

The survey also revealed that approximately half the command uses some type of workstation for over 4 hours a day. These workers use over 30 different software packages on more than 10 different workstation hardware configurations. This scenario presents an upkeep and support nightmare for the ADP Division.

Software standards must be set for the entire command for each type of standard application. These standards must be published and enforced. They should be discussed at ADP Executive Steering Group meetings and other department head meetings so that the intent is clear. Training for the entire command should be planned to orient users thinking to the new philosophy. The Supply Department's help should be enlisted to screen out requests that do not conform with standards or are not adequately justified. Upgrade packages should be purchased only for the standard packages selected. Program packages that will not be supported in the future network configuration and still in use should be phased out. Additional types of software for current applications (i.e. word processing, databases, etc.) should not be purchased or developed without strong justification in writing. If additional software is permitted the standards must be rewritten. The command may want to leave out some of the existing software packages and state that they will be phased out and not supported in the future. This will streamline existing systems, reduce system complexity, and make the IS staff able to respond more readily to user requests for assistance. This will undoubtedly be met with resistance, but it is one of the best ways to bring a distributed computing environment under planned control. It may also decrease upkeep costs in the long run.

A draft Office Automation Plan was sent to the command for further modification to accommodate the evolving situation. This draft plan is included as Appendix C.

At this point 35 people are connected to some type of network. Connecting the remaining command personnel will require the delivery of the equipment that is currently on order and acquiring an additional 30 workstations with future funding. Another pressing need is for additional copies of software packages used by the command to ensure full compliance with copyright requirements. Money has already been set aside for this purpose and a number of software package are on order for various departments.

The survey revealed an large number of tasks that are performed manually that could be automated and information that is passed around the command on paper that could be sent electronically. The ADP Steering Committee should assess these lists from Appendix D and choose several, which if automated, would rapidly reduce manhours spent on administrative tasks.

C. PERSONNEL AND ORGANIZATION

Part of the problem in producing a coordinated command strategic plan for IS lies in the fact that the programmers and analysts are divided into departmental groups, work independently, and have not allocated specific time set aside for communication of plans and work. This is accomplished via informal communications and occasional meetings, but should be formalized, structured into the monthly calendar and made a priority to attend. Another alternative is to bring all of the programmers and analysts together into the IS department again. This proposal would work if the group was placed in a matrix structure working for all departments with a knowledgeable IS manager as the leader. This person should be capable of arbitrating which departments get priority for services based on changes in command level goals and priorities.

The issue of an appropriate IS organization to support various command structures and goals has been faced by many corporations. Case studies have been written on the successes and failures of various corporate IS reorganizations [Ref. 1]. Managing three separate technologies in a coordinated and integrated manner is a new challenge for IS staffs in the 90's. Previous ADP divisions managed only data processing, but the IS staff must now also manage office automation and data communications [Ref. 1]. Pressures for a centralized IS group include more efficient use of resources and personnel, assurance of standards, improved security and planning, and better career paths and training for IS professionals. Priority for these qualities must be balanced with the benefits of a decentralized workforce like better user control and access, improved responsiveness to users, higher independence and creativity for IS personnel, small tailored applications with better fit to field needs [Ref. 1].

At this time the command does not have an officer trained in the details of IS management. A line LCDR or CDR billet should be established to manage IS resources. The billet must be senior enough to be able to deal on an equal basis with the other senior department heads. A civilian in this management position is an alternative, but not preferable due to the culture of the CMWC organization. The command has never had a civilian in a department head or assistant chief of staff position. IS also needs to be made a separate department, not a collateral duty of the Administrative or Supply department head. The ability to evenly distribute and make the most of all IS resources will become more and more critical as budgets and personnel decrease, and more and more functions are performed by automated technology.

Several years ago the Supply Officer billet was P coded requiring a graduate of the Naval Postgraduate Schools Computer Systems Management curriculum. The emphasis for this position evolved toward extensive financial management expertise and became a comptroller position. The operational direction that the command has now taken dictates that a line officer familiar with the mine warfare tactics and operations would now be the best choice to head an IS Department as an assistant Chief of Staff (ACOS). This is especially important in light of the emphasis on development of operational applications such as GOPAS, tactical decision support systems and others described in the CIMP rather than supply related transaction processing applications.

Currently, the primary problem facing the CMWC IS staff is the lack of an adequate number of personnel to accomplish all of the requirements of setting up a distributed network and supporting the variety of applications that have evolved.

Various references suggest workable IS organizations to support distributed computing environments [Ref. 1, 4 & 5]. In general, Reference 4 recommends that installation of equipment, management of databases, and coordination of external support should be centralized, while software maintenance and user support should be decentralized. A suggested organization structure might have an officer as an ACOS heading an IS organization with two teams. One team would contain the technical and network administration personnel, and the other a software maintenance and development support staff that would be the primary customer service point of contact.

D. TRAINING

Implementing training programs for the IS staff and the whole command is extremely important. The best way to reap the productivity gains that a distributed network can give the command is to ensure that everyone knows how to take advantage of its capabilities. When a distributed system is operating properly the IS staff should primarily serve as facilitator for the user driven computing applications [Ref. 4]. This is what is meant by end user computing, a current catch phrase for users developing their own applications with the assistance of IS professionals for support and advice. IS staff members need training that will allow them to help users to analyze their own needs and develop their own solutions.

Initial training for end users should be dedicated to small groups that use a specific application. It should show them how to access shared files on the server, send files from workstation to workstation and attach files to electronic mail. Application training should also include specific tips on how to use the application (word processing, databases, etc.) to create files that will specifically be required at CMWC, and how to utilize macros for repetitive tasks. Training of a general nature can be done on a daily basis via short tips or notes in the Plan of the Day, on the electonic mail bulletin board or at morning departmental meetings. The IS staff should compile a file of short paragraphs on a variety of network use topics.

This type of training also gives the IS staff a chance to remind personnel of correct procedures and policies. Enforcing good security practices is especially important at CMWC, and a major vehicle for improving compliance with a command wide security program is training.

Training will enable the command to take advantage of and progress toward full utilization of what distributed computing has to offer in the realm of reduced paperwork, loss of paperwork in transit and time wasted while personnel hand walk documents around building.

Another area of inexpensive training that should not be neglected are computer symposiums or exhibitions. These showcase new technology and management options. IS professionals will increase their own knowledge, increase their network of professional contacts and return with additional ways to utilize or improve the distributed computing environment. CMWC staff should attend conferences in the areas of network operations, customer support and interoperable software development.

E. PROPOSED DISTRIBUTED COMPUTING ARCHITECTURE

One aspect of planning for CMWC's distributed system that is well documented are the plans for the proposed network architecture. These plans were created and drawn by the network administrator to facilitate the installation of cable. Each department was surveyed for PC, printer and other peripheral requirements and proposed location of the workstations. Cabling was purchased and installed by CMWC IS personnel prior to May 1992.

The onsite interviews with the Chief of Staff and Department Heads revealed doubts about the appropriateness and workability of the proposed network. One of the primary tasks assigned the author was to verify that the proposed network would work to satisfy user requirements and could grow with the command in the future.

The internetworking solution planned by CMWC is one of the simplest and least expensive. The coaxial and unshielded twisted pair cable was inexpensive, and not technologically difficult to install. The straight line Ethernet bus architecture also added to the simplicity of the network and allows for easy expansion or redirection if requirements dictate a change.

The proposed network is displayed in the following diagrams:

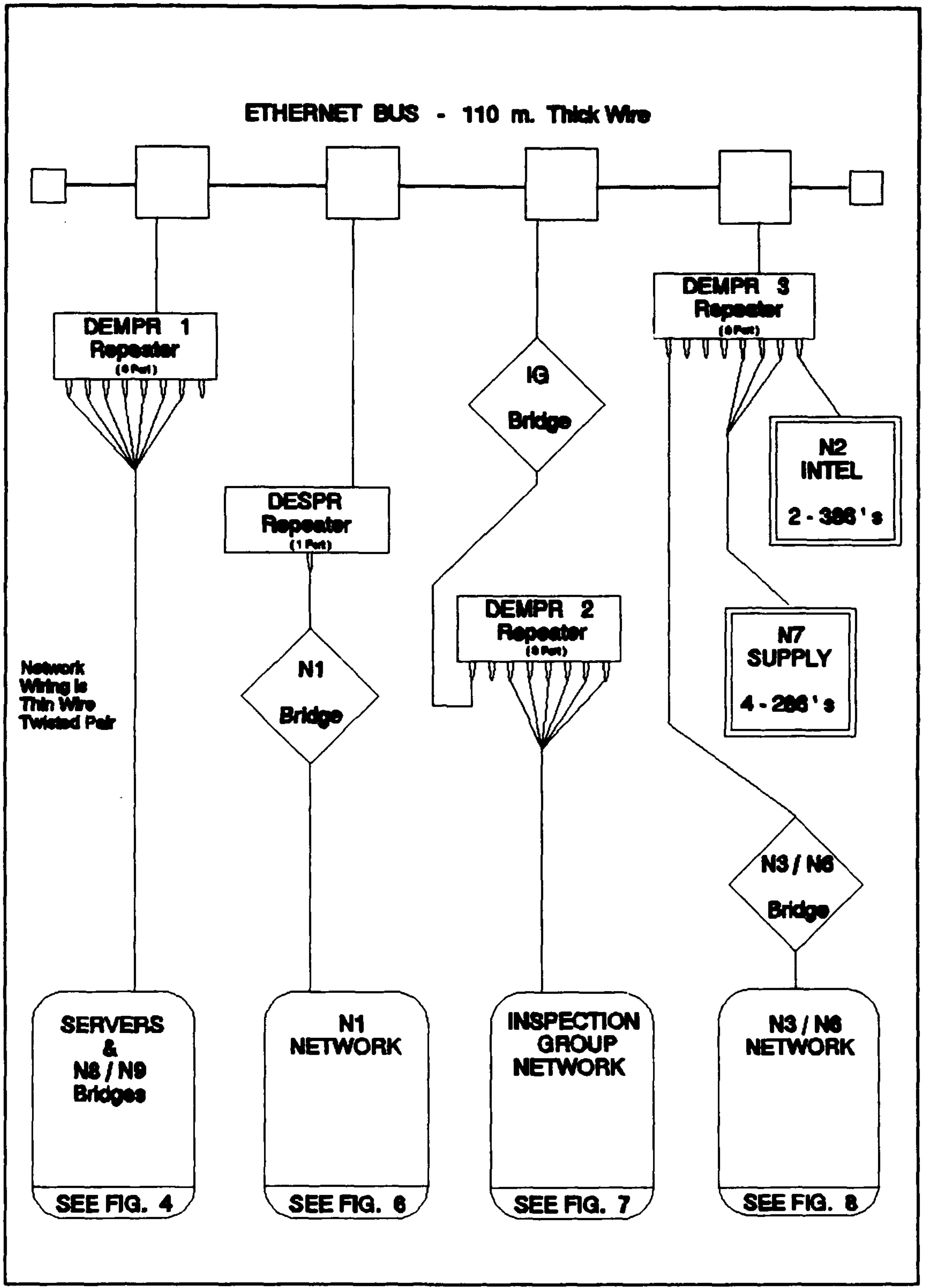

Figure 4: CMWC Proposed LAN Backbone Architecture

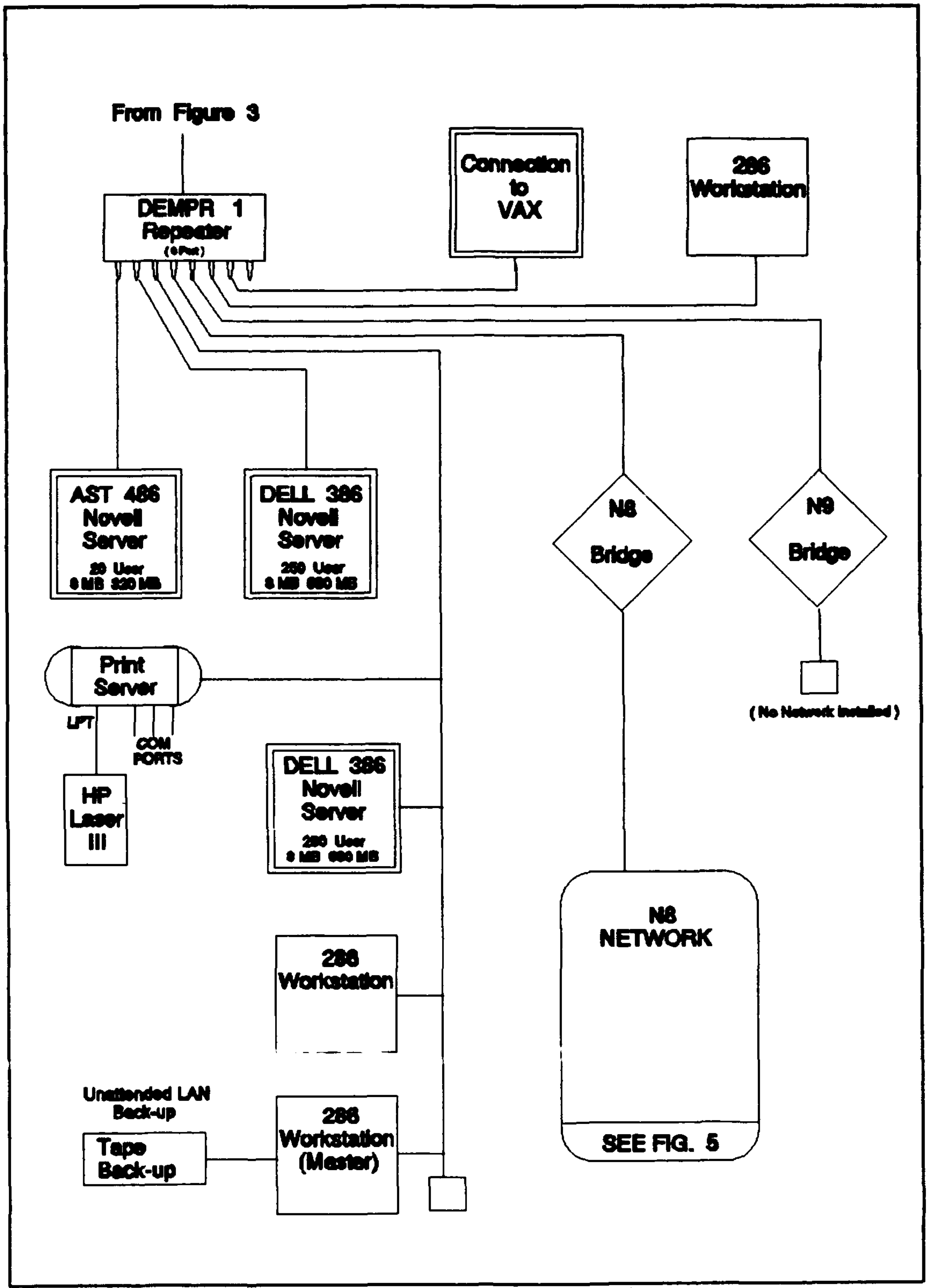

Figure 5: CMWC Repeater 1 Port Connections

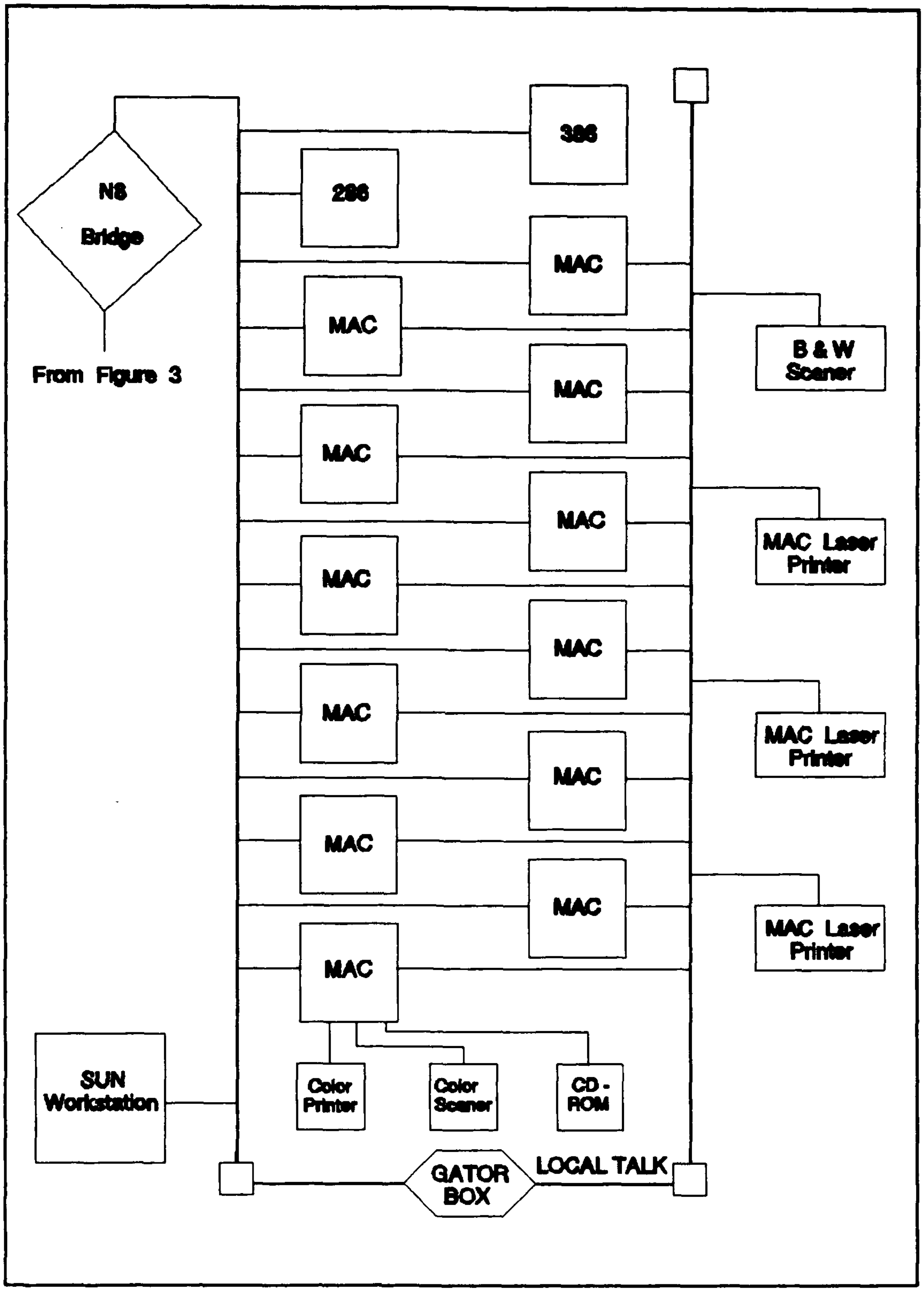

Figure 6: Proposed N8 Department Network

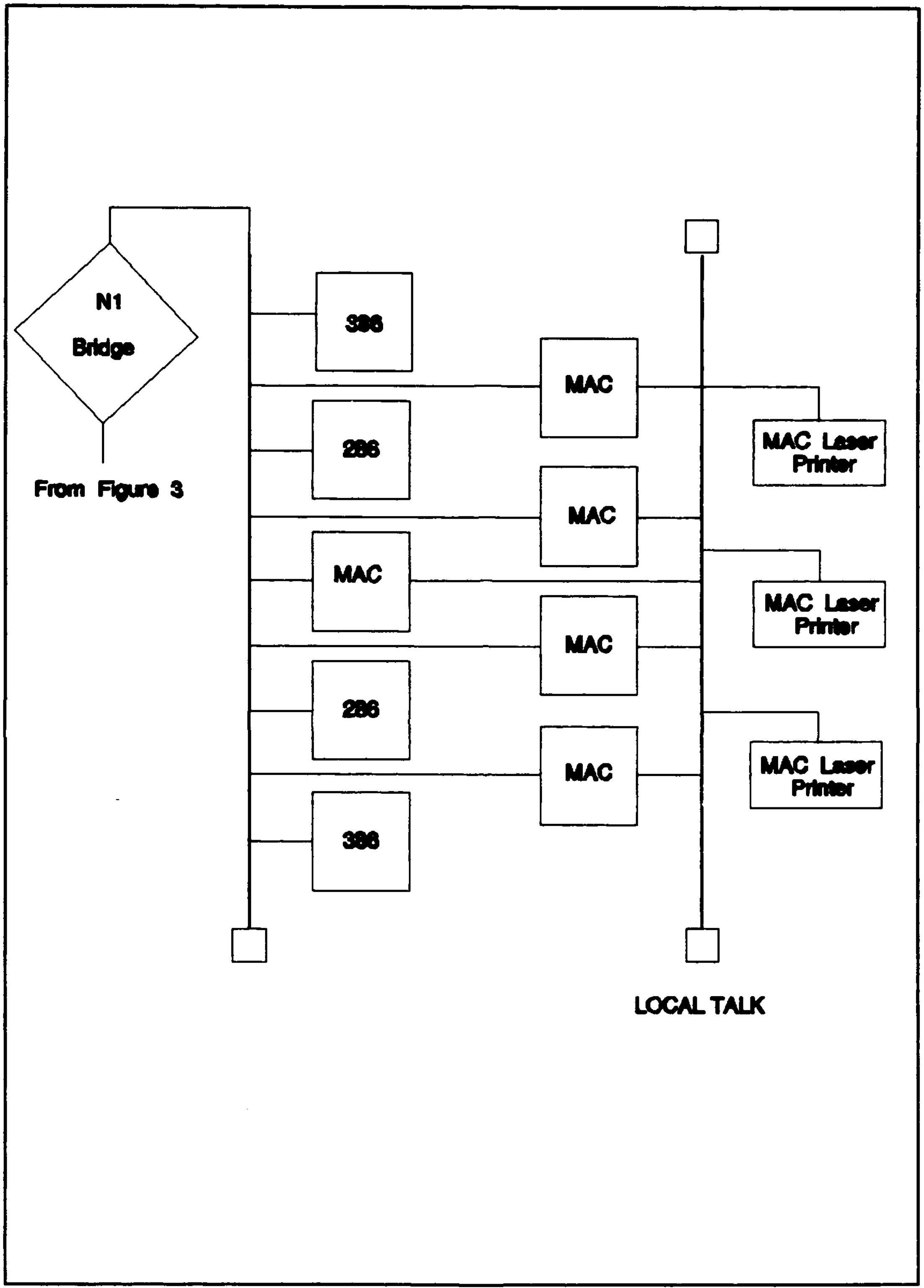

Figure 7: N1 Department Proposed Network Architecture

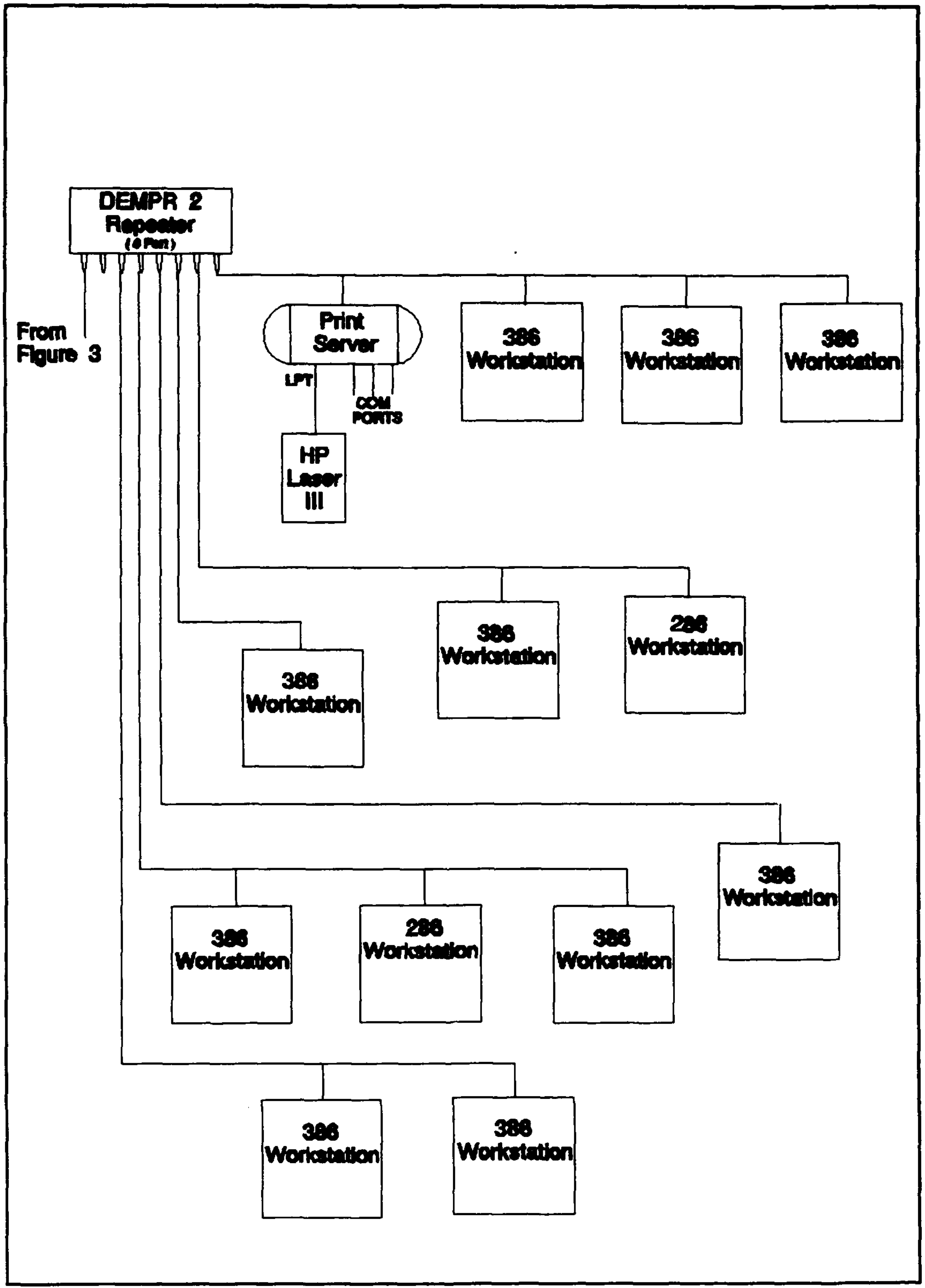

Figure 8: CMWC Repeater 2 Port Connections

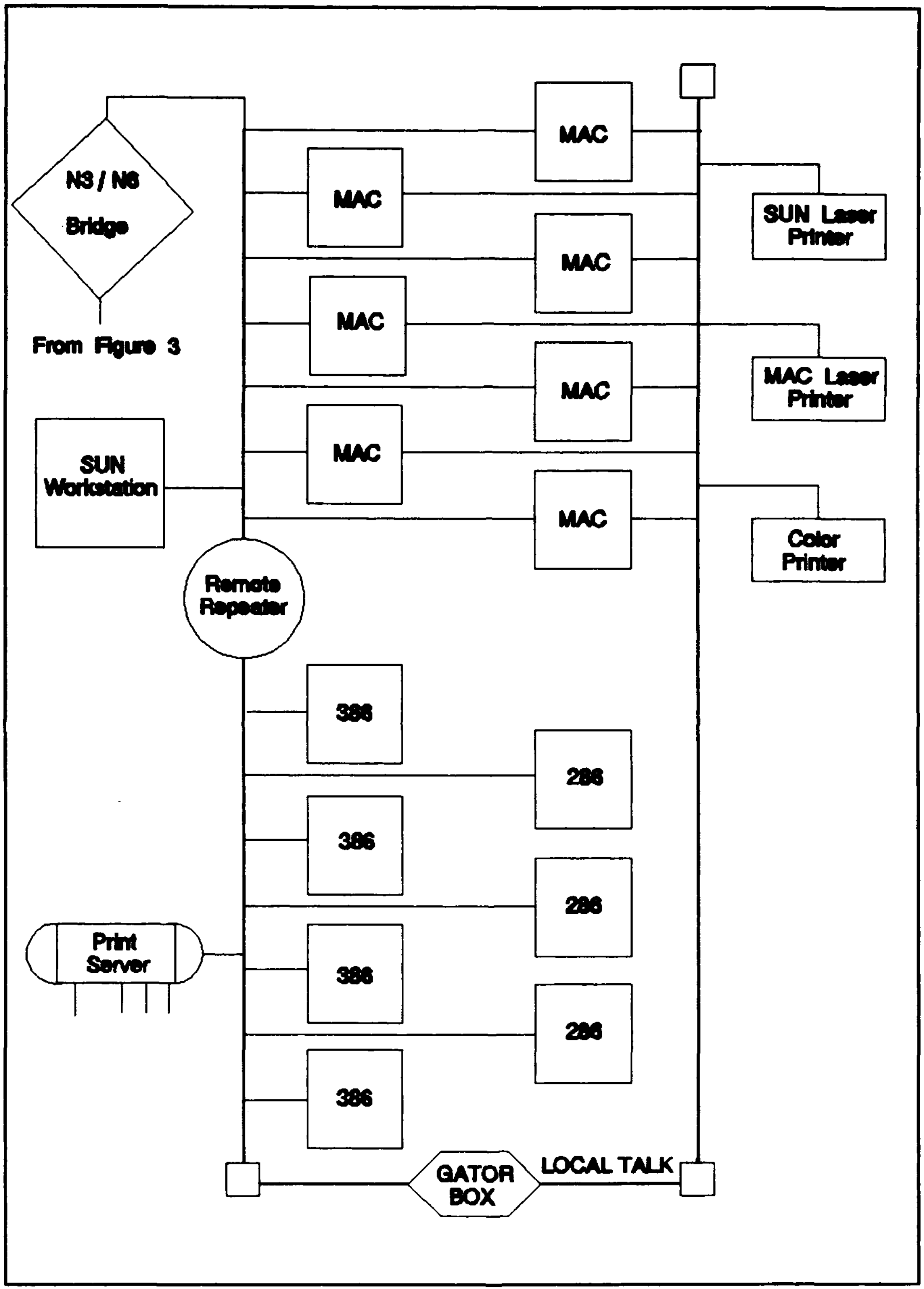

Figure 9: N3/N6 Department Network Architecture

During the onsite visit these drawings were reviewed with the system administrator for completeness and compliance with the OSI Model. The drawings were examined by several experts on network connectivity to insure the plan was feasible based on technology available to interconnect diverse platforms. Alternatives to reduce cost or complexity were researched. The immediate feedback to CMWC was positive, that the proposed network was a viable approach and that they should proceed as planned. Recommendations on improvements and expansion to this network are provided in Chapter V.

The proposed network displays the following client - server environment (Figure 9) to support both centralized and distributed application requirements. CMWC is evolving toward the use of many distributed applications such as email, word processing and scheduling, but must maintain some of their critical databases as centralized applications.

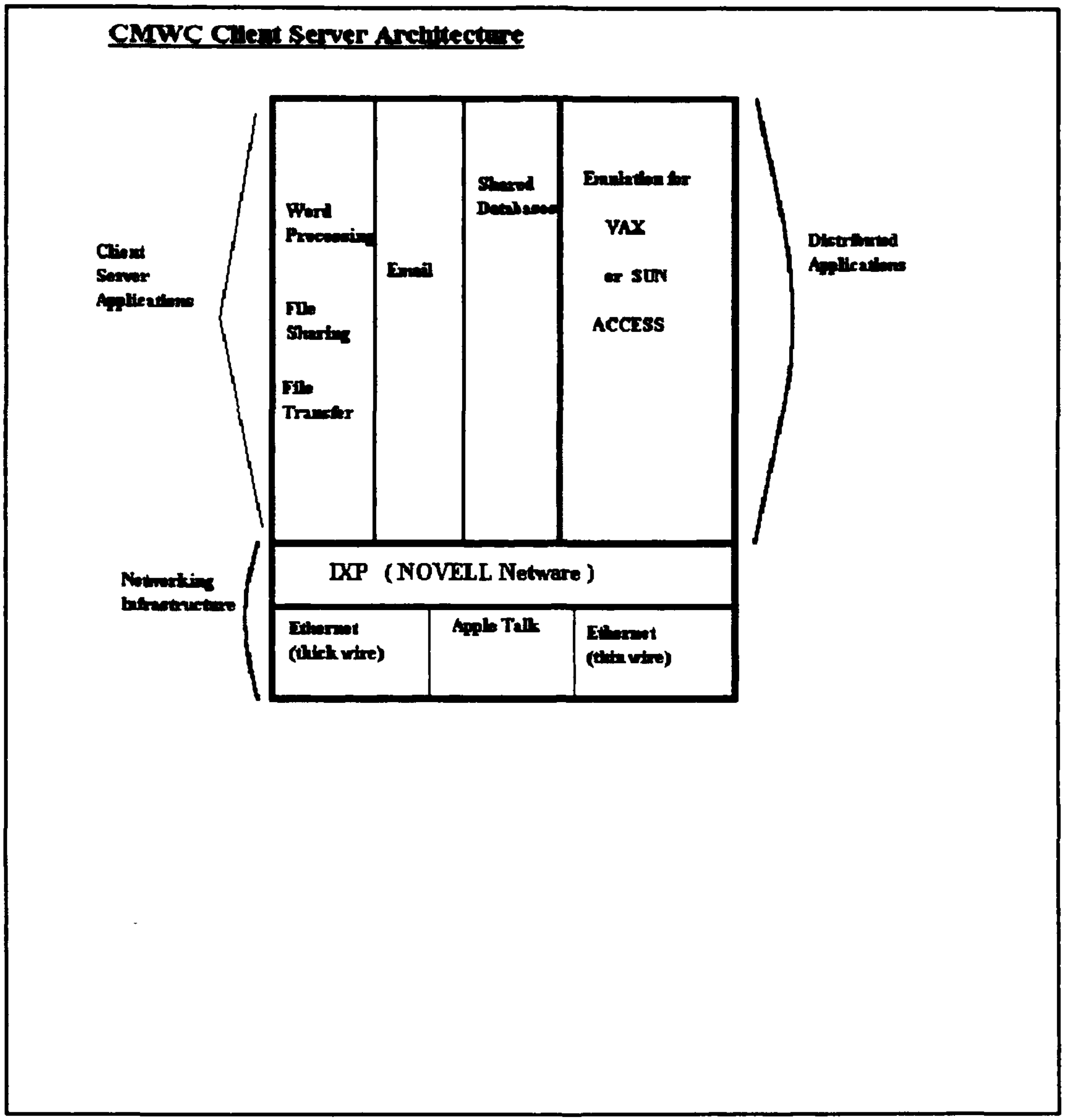

Figure 10: Proposed Client Server Environment at CMWC

Recently, the Ziff Davis test labs undertook a network construction problem for Corporate Computing magazine [Ref. 14]. This project constructed a network almost exactly like the one implemented at CMWC. They tried two approaches, one with a Novell Netware architecture depending on IPX/SPX for internetworking, and the other using a distributed setup with TCP/IP implemented to let the computers communicate. They determined that on a network with these interconnectivity requirements it was "nearly impossible to get a single protocol to work in a large, multiplatform enterprise". They recommend assessing the technologies that you already have, and understanding how new products will connect with the installed base. Both solutions worked for the most part, but the TCP/IP setup cost less and had more features than the centralized one. One complication in the IPX/SPX architecture was tnat VAX users could not access Netware volumes on the server. As long as CMWC eliminates the VAX mainframe and associated terminals eventually, they will not have to confront this problem and their centralized Netware based architecture will have reduced complexity and cost than the example network in Reference 14.

F. SECURITY CONSIDERATIONS

The issue of security is of overriding importance to CMWC. Their original databases on the mainframe are classified and deal with a large amount of classified documentation, files and messages every day. All classified data has resided on the mainframe in a secure space, or in report formats on paper locked in safes each day. The problem that distributed computing presents is the increased spread of the classified data to other media storage types and places, and the increased number of ways to access that storage media. CMWC recently completed drafting a good security plan and appointed a full time ADP security officer.

CMWC's network has been constructed to be secure for information with up to Secret classification. It currently operates in a system high security mode, but needs to evolve to multilevel security. Connection to other agencies or networks is not allowed by workstations or servers on the network. A few individual workstations not connected to the network are configured with modems to allow outside communications and file transfer for specific purposes. One of these is the CAIMS terminal which is required to send mine inventory data to the Ships Parts Control Center in Mechanicsburg, Pennsylvania. Requirements for this type of connection will increase over the next several years. Continuing to transfer required files from the network to the independent PC's via floppy disk is error prone and time intensive. Keeping the network totally isolated is an unrealistic goal, will cause further dependence on paperwork and reduce the positive impact of automation.

An initial method of controlling access to classified data on the network has been solved by ordering Syquest removable hard drives. These will work for some applications such as message drafting and formatting, but not for data or reports from databases too large for the removable hard drive. Also these removable drives should not be requisitioned wholesale for every workstation. The portions of the command like the Supply department and some of the Administrative department that does not deal with classified data will not need them.

Isolating the network and removable hard drives will not solve the future network requirement of interconnectivity with other commands and organizations. The more connections that a network has the greater the productivity possible. A future change to the network architecture that would improve its capability is to separate the network sections into one for classified processes and a second for unclassified. For example, the Supply and Administrative Departments could use the unsecured portion of the network and have a gateway PC to DDN that would allow them to execute file transfers and electronic mail. Other departments would be on a classified section of the network separated by a gateway PC that acts as a firewall to protect the classified data stored on it. DOD and the National Security Agency have not yet approved any specific systems for this purpose, but several are being tested and validated. Reference 15 describes a corporate gateway at Digital Equipment Corporation that works in a manner to protect sensitive information from leaking to the outside yet allows an unlimited flow of data into the organization. The National Security Agency (NSA) has also endorsed a system developed by Motorola called the Network Encryption System (NES) which is capable of securing information up to and including Top Secret. This system runs on a workstation inserted between a group of workstations and a network, and functions as a node on the network. Multiple communities at different security levels can share the same LAN cabling or wide area network facility with unclassified users without the danger of data crossing over from one community to the other [Ref. 16].

Another option for improved network security that CMWC should consider is to convert the network wiring to fiber optic cable. Fiber optic cable is the most secure type of network cabling. It does not emit electromagnetic waves that can be intercepted at a distance, it is not susceptible to interference and it can only be accessed by splicing the cable and adding a termination making it difficult to tap [Ref. 7]. It is currently more expensive than other types of cabling, but the cost is decreasing as the technology is perfected. A future, highly secure network configuration for CMWC would use the new Fiber Distributed Data Interface (FDDI) run to each persons desktop workstation. The Naval Sea Systems Command is currently working on a draft standard for Navy FDDI networks called SAFENET II [Ref. 17]. A large number of systems are being developed using this standard including the first network on a sl.ip, the George Washington Information System aboard CVN-73 [Ref. 18].

G. SOFTWARE CONVERSION

The two mission critical programs that have always operated on the VAX mainframe are being converted to run on Sun SPARC workstations. The conversion of these programs is in progress at the Naval Research Lab in White Oak, Mississippi. There does not seem to be a specific plan of action or delivery date for the converted programs. Command personnel appear to be satisfied with the progress and are not concerned with the lack of a firm completion date. The monetary investment in converting the software is considerable and cannot be carried over from one year to the next. Departments concerned with the use of those programs should track this conversion more closely to ensure that the new programs will be ready before the loss of the mainframe computer. Experience with software conversions shows that they may take twice as long as anticipated due to unexpected complications and changes based on user requests [Ref. 12].

DOD is developing a bad record in the area of software development as described in Reference 13, and creating further examples of poorly executed software management must be avoided.

The VAX mainframe equipment will not be maintained after 1 October 1992 and if it experiences a catastrophic failure access to these programs and their associated databases would end abruptly. Loss of these mission critical programs would initially cause work disruption and require the expenditure of additional funds to repair the mainframe. Another critical concern is the loss of manhours it would cause and the resulting lack of ability to accomplish tasks assigned by higher authority in a timely manner.

V. RECOMMENDATIONS

The following recommendations are based on the status of constructing and implementing a distributed computing architecture at CMWC as of May 1992. They complement and expand on the proposed network diagrams presented in Chapter IV. Many of the required components are currently on order or already in place, but additional funding is available to improve and expand the commands capabilities. The following items would significantly enhance the productivity and usability of the network.

A. FUTURE PROCUREMENT

1. Hardware

a. Servers

The choice of a server platform is dependent on the NOS chosen and the volume of network traffic. A reasonable choice for a file server on a network with a small number of users is a 486DX PC with at least 8MB of random access memory (RAM) running at speeds of 33MHz or above. A critical consideration is how large the hard drive or drives should be to support the applications that run from the server and the volume of files and data stored there. Several servers may be tied together into a single network with each server designed to meet the needs of a particular user group. This design is appropriate for CMWC's command structure. The number of servers will have to be increased as applications are transferred to it from the mainframe.

CMWC's proposed file servers will be adequate initially, but additional equipment should be bought in the next budget year to upgrade to larger hard drives and increased system RAM. The LAN setup should be flexible enough to accommodate changes as users learn to use the network and traffic through the servers gets heavier. As more and more users see productivity gains by the use of electronic transfer the volume of electronic mail messages and files that need to be stored will increase exponentially.

As users become more dependent on the system the issue of fault tolerance must be considered. How will the loss of the network effect daily productivity? If the command decides that they could not stand the failure of a server, they should purchase a fault tolerant server that employs various real-time recovery mechanisms as well as dual components. For fault-tolerant connectivity, network topological design must allow redundancies in links and intermediate systems (e.g. gateways).

CD ROM drives should be purchased for a variety of applications. One should be attached to the main network file server for users to access a variety of CD ROMs published by various government agencies that replace massive paper publications. In particular, supply stock numbers, part numbers and item descriptions are on CD ROM disks supplied by the Defense Logistics Agency. An increasing number of these will appear in the near future containing all types of pertinent reference information. The network should be configured now to take advantage of these benefits.

Another application of CD ROM is archiving. CMWC should begin to transfer its historical files kept on paper or microfiche to CD ROM via flat bed scanners and Write Once Read Many (WORM) drives. Placing historical files on CD ROM makes the information more secure and accessible. Personnel will find that they can consult CD ROM files more quickly than digging through old filing cabinets of supposedly organized files and papers. A task such as this may appear to be too great for current command personnel to undertake given their workload, but might make an excellent project for reserve personnel to implement during a two week active duty period.

If the amount of information that must be accessed on the network from CD ROM becomes extremely large the command might want to consider acquiring an optical drive for the network. These drives are becoming more and more popular for the storage of large databases of historical data. They are constructed like regular disk drives but with platters made of material like CD ROM instead of magnetic coating. These platters hold more information that conventional disk drives or the small diameter CD ROM platters.

Another new and evolving technology becoming prevalent in networking is the emergence of the "super server". A number of companies are now offering what are termed super servers because of their capacity and versatility. Most are running under the UNIX operating system and can be configured to support small or large user groups. One manufacturer's super server can support up to eight Ethernet segments, 120 gigabytes of disk storage and 200 clients. A super server is meant to take the place of the numerous file servers that may be necessary once network utilization increases. The super server's flexible, expandable architecture increases throughput, reliability and capacity, while simplifying data and network management.

b. Workstations

Additional workstations should be purchased for personnel that the current order for 386's and 486's will not cover. These do not need to be fancy machines with large removable hard drives, super VGA, etc, but just basic work machines to satisfy word processing and electronic mail requirements. Every workstation procured from this point on should be ordered with a LAN board that will satisfy connectivity requirements. If possible workstations should be configured exactly alike. This will reduce setup and maintenance time. Each workstation should be configured with the same batch setup files and protected so that users cannot change the settings.

A major emphasis should be to eliminate all of the VAX terminals as soon as possible. This will reduce the upkeep of different types of equipment for the IS staff and will solve the problem of unequal user access to applications that now exists. Some personnel using the VAX terminals still do not have access to electronic mail or the command standard word processing files and application. This is particularly necessary for department heads and senior managers. They should all be using workstations connected to the LAN with CC:Mail capability as soon as possible. The sooner the appearance of managers' desktops appear identical, the quicker compliance with a standard configuration, standard software and a firm network plan will be achieved. The network plan is good and will be flexible enough to accommodate changes, but will continue to be expensive if each person has a different hardware configuration. Keep only those VAX terminals that personnel need to continue existing mission required applications. These personnel need to have access to other workstations where they can read electronic mail. The priority though must be to eliminate the need for personnel to have more than one workstation on their desk. Strive to have all capabilities and applications available to every workstation regardless of its configuration.

More laptops need to be bought because a large number of command personnel travel extensively. If the number of laptops is limited and cannot be permanently assigned to specific people full time, put those available in a pool so that they can be checked out as needed for travel assignments.

Acquiring two more Sun/SPARC workstations would make existing networks in the N3 and N8 departments much more flexible and less prone to down time. The command actually owns additional workstations being used at other support commands. A little pressure to get these back as quickly as possible might save a large expenditure. However, the newer versions of the SPARC stations have incredible power and will be tremendously useful for new and improved graphics applications.

More removable hard drives may need to be bought, but should ONLY be ordered for PC's that will handle classified data.

c. Peripherals

Printers can be a severe bottleneck on user networks. Departments with heavy requirements for printing documents should have additional printers. The setup and configuration of printers can be complicated and changing printer settings for each new user can tie up the pri:ter and personnel for exorbitant periods of time. Printers should be placed with user groups working on similar applications so settings do not need to be changed. Users should not have to leave their work space to retrieve their printed products. Top level managers will find lower cost dot matrix printers attached to their workstations will satisfy their day to day requirements for memo's and reports. This would free up the laser printers for documents that will be sent outside the command. It does not appear there are enough printing assets at present, and this will become a more pressing problem as use of the network increases.

A few additional modems will need to be purchased to support some of the standalone application requirements. These should operate at least 2400 baud and one or two should be procured that have fax capability. At this point the command has one fax machine controlled by its communications staff. More commands are seeing the benefits of fax capability daily and CMWC is certain to have the number of requests for transmission and receipt of paperwork via fax go up. Appropriate security procedures should be written and personnel familiarized with the proper precautions, especially in a command where so much classified information is discussed on a daily basis. Secure modem hardware is being developed by various manufacturers and is another technology in which CMWC should invest in future budget years as the security aspects of the equipment mature and are approved by the NSA. Making the network as fully integrated with outside activities as security requirements allow will be a struggle, but should be a top priority.

2. Software

Upgrading to Novell's Netware 4.0 when it is released is highly recommended. This new network operating system software will have the following features [Ref. 19]:

- The new NetWare Directory Services are designed to support objects across multiple servers instead of the operation of a single server.
- This directory is replicated across multiple servers preventing a single point of failure from causing a total network crash.
- Easier setup of personal accounts with a globally distributed object database.
- Improved installation and usability.
- Enhanced security and auditing features that will implement the required C2 functionality level required by DOD.
- Inactive files on primary storage compressed in the background.

All of these functions will improve various aspects of CMWC's network status or setup.

A variety of new software for easy automated network management exists. CMWC should look into acquiring one of these packages that allow automated setup, autosensing and rerouting around disruptions. Use of this type of utility would eliminate the need for more support personnel as the network grows larger.

CC:Mail Remote packages for laptops would be useful for people who travel to transmit working papers and receive messages and reports from the command. These laptops might have to communicate with a stand alone workstation for security requirements; however, the remote CC:Mail log on does not allow any access to the network itself, but simply transmits and receives the messages in the designated users directory. The problem lies in messages inadvertently containing classified information transmitted over public phone lines or outside access to the network via the server modem.

Additional network and PC security packages will need to be procured and setup on the network to monitor usage and access. Possible PC packages include the Norton Utilities and PC Tools. Higher level security is provided by software like WatchDog and PCDACS. The DOD Automated Information System project office has issued a new publication with approved products complying with the various level of security promulgated by the NSA. [Ref. 20]

B. MANAGEMENT POLICIES

There is currently a significant amount of dissatisfaction within the command about the state of Information Systems support. A wide range of reasons for this were revealed in the interviews. Some of the tension still reflects the past history of the management of IS at the command. A concerted effort on the part of the IS department to level out the amount of support and equipment that each department has will go a long way toward relieving tensions. Setting priorities and increased training on the use of new technologies will also help to satisfy customers needs.

The first step to an integrated network is the replacement of the existing VAX terminals as soon as possible with the 386DX PC's that are currently on order. Especially urgent is the need for management level personnel to have the same electronic mail, word processing, office automation support applications and access. CC:Mail and file transfer cannot be used effectively until all personnel have access to the network. The command should make certain that everyone knows in advance of the new PC's delivery exactly who is going to get the equipment. Any conflict about the number each department will get and their placement will just slow down installation and further frustrate users.

The second priority should be ensuring the network is set up correctly and runs efficiently. The command needs to anticipate that correcting conflicts and answering user questions will take a inordinate amount of time away from productive work and progress toward productivity goals. It may take up to a year before any real gain in productivity is detected by managers.

The training mentioned in Chapter IV is another area that management should insure gets priority. It is sometimes difficult to fit additional training into the work day, but it will eliminate costly mistakes and rework.

In light of the push for Total Quality in DOD, another initiative the command might undertake is talking to all of its customer and supplier commands about how processes might be improved using the new network and its automation capabilities. Joint Process Action Teams (PAT) and Quality Management Boards (QMB) are excellent ways to find new uses for IS capabilities in streamlining processes and improving support. Another facet is to talk to the commands CMWC works with to find out about applications they are developing. A QMB would interact to make certain internal applications would interface effectively with external applications, particularly those which require some type of report or input from CMWC. Compatibility and interoperability are becoming critical throughout DOD, not just internal to each command.

Future support of the network and replacement of equipment as parts age or become obsolete must be considered in upcoming budget years. Right now many of the PC's are covered by initial vendor warranties. A plan should be drawn up now to systematically replace and upgrade a certain percentage of the equipment every year. The cost of mainframe hardware and software upgrades has not really gone away, but instead been replaced by a wider variety of equipment improvement costs. This new network equipment upkeep will require more thought and attention on the commands part to keep it up to date and operable. Right now maintenance contracts for critical equipment should be setup. These vendor contracts should provide replacement equipment on loan while the broken component is repaired.

C. LESSONS LEARNED

A number of the recommendations above were implemented during the past 9 months. Changes were made to the network architecture as new possibilities and cost savings presented themselves. CMWC now has an operating network with some distributed processes and is beginning to see the benefits of electronic communication and file storage. Further evolution of the system and its users will depend on training and management attention to cultivate an atmosphere of the strategic importance of the networks positive uses.

The following items were prominent lessons learned compiled by the command and the author by late 1992.

- The need for an ADP Steering Committee to assist with the integration of communications, and discuss plans and alternatives.

- There needs to be a way to disperse information easily throughout the command about the plans formed by the steering committee so that all hands know what to expect during the conversion process.

- An equal level of knowledge throughout the command is critical. Unequal levels lead to tension and distrust of the IS staff and the technology they are trying to implement. Knowledge of what is planned leads personnel to feel like they are a part of the process and not a victim.

- Preplanning to arrange dedicated personnel for quick installation of new equipment when it arrives. Customers should be briefed so that they know personnel will not be available for other tasks after a delivery of equipment.

- The conversion of the word processing files on the VAX took much longer than expected. The actual process to convert files from a mainframe format to DOS needs to be well known in advance, and specific time and personnel set aside to accomplish the task once the equipment is in place. Reserve personnel were used to help complete this task.

- The required placement for PC's in various departments changed during the period of time the equipment was on order. When the equipment arrived users wanted PC's located in areas where cabling was not available based on the original plan and departmental requests. A command reorganization had moved personnel and job tasks. Any upcoming command changes must be taken into account for cabling and network design.

- The removable hard drives were even more useful than anticipated. The hard drives have helped to compartmentalize information and keep it better controlled than on pieces of paper. For instance, the watch section was able to draft classified messages after hours and then secure the drive in a safe.

- The command did not order enough printers to support the number of personnel that started to use the network for word processing. Overestimating printer requirements initially and budgeting for it will prevent the bottle neck of too many users sending print jobs to the same printer.

- The capacity of the hard drives on the files servers is filling up quicker than expected. Budget for twice the size of hard drive than what is originally thought to be needed. This is particularly true if new software is bought to be shared on the file server. The newer software packages take up to 20 MB's of storage each. Workstations also needed larger hard drive capacity than anticipated and some needed to be upgraded almost immediately.

- The item affecting the entire conversion most prominently was procurement problems. The lag time between placing the order and the delivery caused almost all of the equipment to be technically obsolete by the time it was delivered. An expedited procurement process would improve all facets of conversion and user satisfaction with the result. Another aspect of the procurement system impacting negatively on CMWC's plans was that groups of equipment were procured by different buyers at different times. The equipment delivered was then configured differently and in some cases totally incompatible. Several pieces were of poor quality and had to be exchanged or returned.

Commands anticipating future conversions should be on the lookout for methods to avoid these pitfalls. An initial discussion with the personnel that will be doing the procurement is particularly important. Well written and specified open purchase documents should be thoroughly screened to make certain all compatibility requirements are laid out and the buyers understand the criticality of the purchase and delivery of exactly what was specified. Working with the buyers on a weekly basis maybe required to clarify specifications and ensure the correct equipment is purchased in a timely manner.

If the budget allows, it is sometimes best to hire a System Integration specialist such as Anderson Consulting or Electronic Data Systems (EDS) to deliver a coordinated package of hardware and integrated network technology. Reference 21 describes snme of these companies and their strengths/specialties. Self help conversions such as CMWC undertook cost less but can take a larger toll in time and patience for the personnel at the command involved.

Future research and thesis topic possibilities exist at CMWC. The command will be moving to Engleside, Texas late this year and must plan both temporary and permanent information systems installations to support their ever increasing mission requirements. A documented plan for their new permanent building would help to justify expenses and articulate the direction future IS support will take. Other thesis possibilities exist in any of the areas of software development for geographic positioning data bases, operational support and decision support systems for mine warfare.

APPENDIX A: QUESTIONNAIRE

The following questionnaire was distributed to all command personnel three days before the first onsite visit. Questionnaires were collected by the Administrative Officer and reviewed after the interviews were conducted.

INFORMATION SYSTEMS SURVEY

1. WHAT DEPARTMENT DO YOU WORK IN? ______________________________

2. Do you use a personal computer, computer terminal or typewriter to do your job anytime during a normal work week?
   (circle one) YES NO

3. If you do not use any of this equipment or any other type of data processing equipment please skip to question 14.

4. If you use a typewriter, what do you type? (circle all that apply) FORMS LETTERS ENVELOPES REPORTS
   MEMO's MESSAGES OTHER ____________________

5. How many hours per day on an average workday do you use this typewriter? (fill in the blank) ________________________

6. If you use a personal computer what type is it? (circle all that apply)
   IBM or Clone with DOS XT AT/286 386 486
   IBM or Clone with UNIX XT AT/286 386 486
   SPARC Workstation
   Sun Workstation
   Macintosh
   Other ________________________________ (describe)

7. How many hours per day on an average workday do you use this personal computer? ______________________________

8. If you use a computer terminal connected to the VAX mainframe, how many hours a day do you use this terminal? ____________________

9. If you use a computer terminal connected to the mainframe what types of programs/applications do you use? (circle all that apply and state name of program)

Word processing/Text Editing____________________
Financial/Spreadsheet____________________
Database____________________
Report Generation____________________
Electronic Mail____________________
Special Mine Warfare Program ____________________
Other____________________

10. If you use a personal computer, SPARC/SUN workstation or a MAC what types of programs/software applications do you use? (circle all that apply and state name of program)

Word processing/Text Editing____________________
Financial/Spreadsheet____________________
Database ____________________
Graphics____________________
Desktop Publishing____________________
Report Generation____________________
Electronic Mail____________________
Special Mine Warfare Program ____________________
Special Utilities____________________
Other____________________

11. If you use a personal computer, SPARC/SUN workstation, or Macintosh is it connected to others in a network?
(circle one) YES NO

12. Do you work with classified data/documents?
(circle one) YES NO

If so, are the data/documents stored on a computer?
(circle one) YES NO

13. If you use a personal computer with its own hard drive how many megabytes of memory does it have?
(circle one or fill in the blank)
20MB 30MB 40MB 60MB 80MB 100MB other__________
How much memory on the hard drive is free?__________
The easiest way to answer both of these questions is to go to the DOS prompt (C:>) and type the command CHKDSK. The answer to the first question is: # bytes total disk space. The answer to the second question is: # bytes available on disk.

14. Are there any job tasks that you currently perform manually that you would like to see automated/computerized? (describe briefly)

15. What type of information do you currently pass to or receive from other personnel/departments on paper or in some form of printed report?

APPENDIX B: INTERVIEW QUESTIONS

Questions for Department Heads

1. What is your departments name? Mission? Functions? Duties? Total # of personnel?

2. What additional computing ability would you like for your department to have? (given no time or $ limits)

3. What do you do now manually that might be automated? What type of records are stilled stored manually in records or file cabinets?

4. What additional duties or missions will your department be assigned in the next year? next five years? in Texas?

5. What do you dislike about your current computing setup? What is too hard or frustrating for workers? Repetitive?
   Manually entered data?

6. Vision of the direction that CMWC is going?

7. Ideas, plans for future growth? Future support functions?

8. What capabilities do other departments have that you would like to have for yours? Why?

Questions for Departmental Info Systems Specialists

1. What computer hardware are you responsible for/does the department use?

2. What computer software does the department use? Develop?

3. What type of network do you have?

   Network software?

   Connections to mainframe or other networks?

4. Specific current architecture by department:

   HW, SW, servers, shared printers, protocols, modems

   Any departmental equipment not used by a specific individual

APPENDIX C: OFFICE AUTOMATION PLAN

The following text was suggested as a draft office automation plan for the command. This plan covers the basics for a network office automation plan. The key idea is to document status and plans for future reference with which to compare new ideas and technology issues that arise (i.e. does the new idea proposed fit with our plan or will it require a lot of work to make it productive?). This is a method to limit the types of software and hardware procured without departmental territorial issues coming into play. It is critical to the success of a command network to eliminate a "mine and theirs" mentality. The Supply Officer must buy into this idea and help to enforce procurement requirements. The attached text may be issued as a command instruction, notice, or plan with a cover letter signed by the Commanding Officer.

A. BACKGROUND

The area of Office Automation (OA) is progressing as rapidly as other areas of Information Systems technology. As with any evolving technology, many paths are available to pursue. Specifically, a comprehensive, unified Office Automation strategy for CMWC is required. This plan will allow CMWC to proceed expeditiously as it strives to take advantage of Information

Systems technology, to increase productivity, and to reduce paperwork. The plan documents where office automation has been, where it is currently, and presents an intended path to pursue at CMWC.

B. PAST ENVIRONMENT

Several years ago, OA was solely secretarial word processing with document archiving. During this period, specialized word processing systems, such as the VAX All-in-One word processing system and manual typing were used. This system provided dedicated, dumb terminals as input devices, mainframe disk and tape for document archiving, and standard line printers or typewriters as output devices. Users needed to define and provide any other services required. The terminals for word processing were used in addition to terminals for specialized programs linked to other mainframes. This required multiple devices on user desktops to support multiple applications.

The VAX All-in-One system also provided electronic mail, calendar, time management, and various other utilities for users. Unfortunately, these processes could only be shared among users with this type of terminal. Since not all personnel at CMWC had a VAX terminal on their desk the effectiveness of these services for command coordination was limited.

C. PRESENT ENVIRONMENT

During the mid 1980's, some of the user community migrated to using Macintosh computers for graphics applications, and IBM compatible Personal Computers (Pcs) due to their availability under the DESKTOP III contract. These workstations provide a single device to perform multiple applications (that is, terminal emulation for the VAX mainframe, office automation requirements, specialized user applications, etc.). Typically, these PCs connect to the mainframe via an Ethernet Local Area Network (LAN) and thus provide a peer-to-peer cooperative environment.

The office automation services at CMWC are provided on intelligent, multi-function PCs (Macintosh workstations, IBM compatible 286, 386, & 486's and Zenith 248's predominantly). With these PC's users can access electronic mail, time management, spreadsheet, word processing, personal database management, and graphics on a suite of standard software applications. Terminal emulators provide connectivity to the VAX mainframe while it is still in use. The LAN provides connectivity between various department networks and to the primary file servers. High quality printer support from laser and color printers, and high volume storage are provided on the LAN. Facsimile machines operate in several departments in a stand alone mode.

D. SOFTWARE STANDARDS

The following are the suggested standard packages for various applications required for office automation. The departmental programmers and analysts will provide support for the daily use of these off the shelf packages, and create specialized programs within these applications for mission specific requirements at CMWC. Programmers and analysts will not support the use of software packages other than those listed. These standard software packages will be the only software procured at CMWC. Upgrades to these packages will be authorized for procurement as required by mission needs. Exceptions to this policy will require a well documented Abbreviated System Decision Paper (ASDP) for justification, stating specifically why one of the standard packages is not adequate, and detailing initial and future upkeep funding requirements for that package.

Application	Software Package
Executive Desktop Support (IBM)	MS WINDOWS
Executive Desktop Support (MAC)	MAC WINDOW SYSTEM
Executive Desktop Support (UNIX)	XWINDOWS
Electronic Mail(internal)	CC:MAIL
Electronic Mail(external)	DDN (SMTP)
Menu/File Management System	Windows
Time Management	Calendar Maker
	Net Scheduler

Word Processing	Word Perfect
Writing Assistance	Grammatik
Message Formatting	MTF
Spreadsheet	EXCEL
Specialized Printing	Sideways
Database Management	DBASE III
Mac DB Development	FOURTH Dimension
Project Management	TIMELINE
Graphics	ALDUS Persuasion
	Pixel Paint
Desktop Publishing	Pagemaker
Computer Aided Design	AutoCad
Communications	PROCOMM PLUS
Screen/Text Editor	PC-WRITE, DOS 5.0 Shell Editor
Utilities	Norton Utilities
Virus Protection	Anti-Virus
Terminal Emulation	(VAX Emulation Program)
Network Software	Novell Netware 3.1

At the executive, managerial, supervisory, and some clerical workstations Windows is used for full spectrum desktop support. This package provides an electronic desk environment with a menu, notepad, calendar, to-do list, phone directory, and calculator. The icon based menu system provides the user with a single-key approach to application selections. The network file server designated as a directory on user machines allows various departments to place critical reports and information into a multiuse package for viewing and decision making.

CC:Mail is the electronic mail package used for general messaging and correspondence throughout CMWC. It is available to all PC's and Mac's connected to the network. ASCII files may be attached to messages and transmitted on the network reducing the requirement for copies and passing of paperwork. For external mail, SMTP will be used across DDN. Together, users can process electronic mail locally, organization wide and externally.

For time management, we are installing NET SCHEDULER II a LAN-based application. This package provides calendaring and appointment notification as well as conference room management. Especially important is this program's ability to send appointment notifications automatically through CC:Mail providing additional capability and convenience.

Our command standard, and a Navy wide standard, for word processing is WORDPERFECT. PC-Write or the DOS 5.0 Editor, ASCII file full screen text editors, are used as program development. For spreadsheets, we use Microsoft EXCEL supplemented with Sideways for printing extended format data. The personal database standard is DBASE III Plus for IBM compatible PC's and Fourth Dimension for Macintosh applications. These applications reside on workstations where required or requested by the functional groups or departments. Users may exchange files via attachment to electronic mail messages or via LAN file servers.

PC disk/recovery utilities are available via the Norton Utilities. Floppy and hard disk management requires a tool to recover deleted files and manage disk space. Novell's Netware is used to manage the Ethernet LAN, establish connectivity and access to information and printing capabilities.

Graphics preparation capabilities for informal and formal presentation or animated video are created in Aldus Persuasion or Pixel Paint. For computer aided design applications, our design office uses AUTOCAD. Pagemaker is used as a Desktop Publishing tool.

Procomm Plus will be used on standalone workstations (not connected to the secure LAN) for use with modems to access other commands data systems. Specific mission requirements dictate the requirement to connect to and transmit information to external commands.

CMWC's strategy for software use on the file servers is strictly for data sharing/saving and printer sharing. The option of buying LAN versions of all PC software is not deemed in the best interest of CMWC. LAN versions of software installed on file servers with multiple users would cause one point of failure to disable many users at the same time. CMWC will procure the standalone versions of software for key business requirements for individual departments to preclude this occurring and eliminating the economic/productivity threat of one point failure. For less critical software, LAN or site license versions are an economical option that will be used.

Further procurement of "Word Perfect Library" for use as a menu system is no longer authorized. (The paragraphs above should also be used to limit use of particular packages to certain segments of the command if necessary.)

E. HARDWARE STANDARDS

Standard IBM compatible personal computers and advanced Macintosh workstations will continue to be procured and used at CMWC with a few exceptions as detailed below. All dumb terminals will eventually be phased out and replaced with PC's or Macintoshes depending on the required uses of the workstation. Removable hard drives are used on only workstations that store classified data. All workstations acquired will have LAN access capability.

High quality printer support and high volume local storage are provided through the print and file servers on the LAN. There are currently 2 servers for this purpose. These servers support the user community by functional groups. One IBM compatible 486 and one 386 with 200M byte SCSI hard disks handle file server functions.

Two departments use Sun/SPARC workstations as servers and program development platforms for their specialize requirements. An additional SPARC station will serve as a data backup device and be available for use should the main workstation go down.

F. REQUIREMENTS TO COMPLETE ENVIRONMENT

Recent reorganization of CMWC has changed and increased the need for workstations with office automation capabilities. Acquiring the responsibility for operational units heightens the requirement for expeditious handling and routing of correspondence. We now need workstations in areas that have increased in size, or changed their mission responsibilities. Resources have been shifted to respond to these changes, but more are required. At this time more workstations are required to replace existing dumb terminals. The Supply Department has been tasked to procure and provide these replacements as rapidly as the budget climate permits. Existing workstations require the installation of LAN boards and software to allow access to the LAN and CC:Mail.

To further enhance CC:Mail response time and general file access another file server is to be installed and the user community divided between the two. This will do two things: (1) provide improved response time by having fewer users per file server; and, (2) provide fault tolerance in that not all users would not be down should file server be inoperative.

During the initial survey of CMWC for software requirements, it was found that additional copies of standard software are required to provide legal copies to all users. Lists of these requirements have been consolidated and procurement initiated.

Training must be developed and provided to users. Although most users have had DOS and cc:Mail training, additional network training must be developed and provided to support the use of file exchanges within work groups, and among different work groups, via the file servers. This training must encompass the ability to attach files to CC:Mail messages and to use LAN commands to access file and print servers. It is important that this training include procedures unique to each of the standard OA applications that are supported at CMWC. Software tutorials for standard packages will be placed on the file server for access by all users so that they may learn the capabilities of various packages at their own pace. Training may be the single most important key to the success of an OA strategy, in as much as its success is the increased productivity of the user community and CMWC as a whole.

To recognize productivity gains from all the equipment and software available today, the Information Systems Section will be organized to provide technical personnel to work with various groups in an effort expedite the use of this technology. With the end-user playing the most significant role, applications and procedures will be developed to increase productivity and allow "more work with less people".

(Document any changes to the ADP support staff in this paragraph that are required to support the network architecture and the office automation.)

(Document any other specific requirements to complete your initial network and office automation setup in this area.)

G. PLANS FOR THE FUTURE

Every day, advances are made in office automation hardware and software. Add to that advances in networking technology, and any plan will be antiquated in a short time. The initial OA plan for CMWC is no exception. Objectives will be refined and updated to use the most current technology.

Additional methods to handle the transmission of classified data must be researched. The use of secure modems and LAN connections would reduce the network management time. Upgrades to the network cabling should pursue a fiber optic desk access network due to its excellent security capability.

(Document ideas and plans for the future in this section. Just putting them on paper will go a long way toward getting funding in future budget years. If cost data is available include the specific numbers in this section. THINK GRANDLY! This is the area to document the dream!)

Any plan of this nature is subject to change and growth. This document will be updated when major changes in the direction of the total system architecture are foreseen. Hopefully, this will also be a platform from which other ideas and areas of development will spring. The CMWC Information Systems Section will continue to keep abreast of evolving IS technology and strive to implement the best products and time/manpower saving ideas.

APPENDIX D : MANUAL JOB TASKS

The following list of manual job tasks currently performed that might be automated at CMWC was compiled based on answers to question 14 of the command survey (Appendix A).

Travel Orders
Trip Requests
Trip Reports
Future Schedules
Message Reading
Accounting and Budget Reports
Various Memo's
Requisition Preparation
Obligation Preparation
Receipt Processing
Forms for Awards
Fitness Reports
Evaluations
Plan of the Week
Placement Personnel Tickler
Chart Inventory
Correspondence Transmittals
SNDL Program

These items were suggested in answer to survey question 15 as information that is currently passed through the command on paper that might be distributed or routed electronically.

Memorandums, Letters, & General Correspondence
Ships Schedules
Travel requests
Faxes
Route Survey Data
Plots
SORTS/CASREPS
Training
Personnel Schedules - Leave, TAD, etc.
Status of Travel Funds
Answers to Queries
Requisitions
Financial Data and Reports
Photographs
Minor Property Custody Records
Clearance Lists
Instructions, Notices & NWP's

LIST OF REFERENCES

1. Cash, James I. Jr., et al., Information Systems Management: Text and Cases, 2nd Edition, Irwin, Homewood, Illinois, 1988.

2. Buchanan, Jack R., and Linowes, Richard G., "Understanding ◌istributed Data Processing", Harvard Business Review, July - August 1980.

3. Buchanan, Jack R., and Linowes, Richard G., "Making Distributed Data Processing Work", Harvard Business Review, September - October 1980.

4. Leigh, W. E., Distributed Intelligence: tradeoffs and decisions for computer information systems, South-Western Publishing Co., 1987.

5. Martin, J., Design and Strategy for Distributed Data Processing, Prentice-Hall, Inc, 1981.

6. Commander Mine Warfare Command, "Component Information Management Plan (CIMP)", September, 1991.

7. Stallings, William. Data and Computer Communications (2nd ed). Macmillan, New York, 1988.

8. Johnson, R. E. and Peterson, S. W., "Study of the Naval Military Personnel Command: Internet Issues, Requirements and Recommendations", Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1990.

9. Federal Information Processing Standard 146: Government Open Systems Interconnection Profile, National Bureau of Standards.

10. Open Systems Foundation, Inc., "Introduction to Open Systems Foundation Distributed Computing Enviromnent", Prentice Hall, 1992.

11. Janusaitis, Robert, "Meeting the NOS selection challenge", Network World, 12 October 1992.

12. Kitfield, James, "Is Software DOD's Achilles' Heel?", Military Forum, July 1989.

13. "DOD Automated Information Systems Experience Runaway Costs and Years of Schedule Delays While Providing Little Capability", Sixth Report by the Committee on Government Operations, House Report 101-382, U.S. Government Printing Office, Washington, DC, November 20, 1989.

14. Longsworth, Elizabeth, & Montgomery, John, "Network Puzzle", Corporate Computing, January 1993.

15. Ranum, Marcus J., "A Network Firewall", Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, MD, 12 June 1992.

16. "Navy Policy on the Motorola Network Encryption System (NES)", Chief of Naval Operations letter dated 22 April 1992.

17. MIL-HDBK-818-1, "Safenet Network Development Guidance", Space and Naval Warfare Systems Command, Code 231-2B2, Washington, DC, 20363-5100.

18. R. Kochanski and J. Paige, "SAFENET: The Standard and Its Application", IEEE LCS Vol. 2, No. 1, New York, NY, pp. 46-5 1 , Feb. 1991.

19. Chernicoff, David P., "NetWare Casts Shadow Over NT", PCWEEK, Volume 10, Number 3, 25 January 1993.

20. National Computer Security Center, "Information Systems Security Products & Services Catalog", Government Printing Office, 1993.

21. Weston, Rusty & Wilder, Clinton, "Partners in Profit", Corporate Computing, March 1993.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Commander, Mine Warfare Command ATTN: N1 Charleston Naval Base Charleston, SC 29408	2
4.	Lane L. Pritchard Supply Office USS McKee (AS-41) FPO AP 96621-2620	1
5.	Kishore Sengupta, Code AS/Se Naval Postgraduate School Monterey, CA 93943-5000	1
6.	Myung Suh, Code AS/Su Naval Postgraduate School Monterey, CA 93943-5000	1